UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA:
INGENIERÍA ELECTRÓNICA

Trabajo de titulación previo a la obtención del título de:
INGENIERA ELECTRÓNICA

TEMA:
SISTEMA DE GESTIÓN UNIFICADA DE AMENAZAS (UTM) EN LA FUNDACIÓN PARA EL DESARROLLO INTEGRAL ESPOIR

AUTOR:
ADRIANA ELIZABETH YÁNEZ TAPIA

TUTOR:
JHONNY JAVIER BARRERA JARAMILLO

Quito, septiembre de 2020

CESIÓN DE DERECHOS DE AUTOR

Yo Adriana Elizabeth Yánez Tapia, con documento de identificación Nº 050313562-6, manifiesto mi voluntad y cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autora del trabajo de titulación intitulado: "SISTEMA DE GESTIÓN UNIFICADA DE AMENAZAS (UTM) EN LA FUNDACIÓN PARA EL DESARROLLO INTEGRAL ESPOIR ", mismo que ha sido desarrollado para optar por el título de: Ingeniera Electrónica, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en mi condición de autora me reservo los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

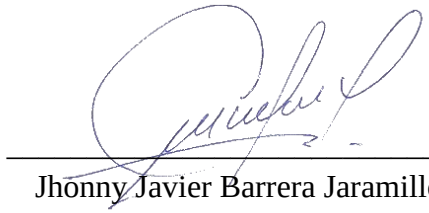
Adriana Elizabeth Yánez Tapia
Cédula: 050313562-6

Quito, septiembre de 2020

DECLARATORIA DE COAUTORIA DEL DOCENTE TUTOR

Yo, Jhonny Javier Barrera Jaramillo, declaro que bajo mi dirección y asesoría fue desarrollado el trabajo de Titulación: "SISTEMA DE GESTIÓN UNIFICADA DE AMENAZAS (UTM) EN LA FUNDACIÓN PARA EL DESARROLLO INTEGRAL ESPOIR", realizado por Adriana Elizabeth Yánez Tapia, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana para ser considerados como trabajo final de titulación

Quito, septiembre de 2020



Jhonny Javier Barrera Jaramillo
Cédula: 1400378475

DEDICATORIA

Quiero dedicar esta tesis primeramente a Dios por las bendiciones derramadas.

A mis padres y hermanos por apoyarme siempre y ser mi mejor ejemplo de lucha y perseverancia. A mi esposo por todo el amor y apoyo incondicional, por ser mi guía y quien me ha empujado a salir adelante en los momentos difíciles. A mi amada hija, por ser mi luz, y por ser ese regalito de Dios que me inspira y motiva cada día y me hace tan feliz.

A todas las personas especiales que me acompañaron en esta etapa, aportando a mi formación tanto profesional y personal.

AGRADECIMIENTO

Me gustaría agradecer en estas líneas primero a Dios y las personas espirituales que me han acompañado siempre, por darme fuerza y salud para llevar a cabo mis metas y objetivos y permitirme llegar a este momento tan importante de mi formación profesional.

A mis padres Milton y Mercedes, mi mayor orgullo, por apoyarme siempre y por haberme forjado con valores y principios que me han permitido ser la persona que actualmente soy, y por todo su cariño y amor absoluto.

A mi esposo Javier, por todo el apoyo incondicional brindado durante todo este tiempo juntos, por impulsarme siempre a conseguir mis metas, gracias infinitas por tus consejos, amor y paciencia, y por acompañarme en este camino de vida y de sueños. A mi querida hija Samantha, por todo el amor, dulzura y felicidad que nos entregas todos los días, y por los momentos que hemos sacrificado juntas.

A mi tutor, Ing. Johnny Barrera, por haberme orientado no solo en la elaboración de este trabajo de titulación, sino por todas las enseñanzas a lo largo mi formación profesional, por su apoyo incondicional y sus palabras de aliento, más que un docente ha sido un amigo.

A la Universidad Politécnica Salesiana y los docentes, principales protagonistas de mi formación profesional.

A la Fundación para el Desarrollo Integral ESPOIR, y a todos los que son participes del Departamento de Tecnología por ser percusores y facilitadores de este proyecto.

A mi familia, hermanos, tíos, primos, amigos lejanos y cercanos, que con sus oraciones, consejos y palabras de aliento hicieron de mí una mejor persona y de una u otra forma me acompañan en todos mis sueños y metas.

ÍNDICE GENERAL

INDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

De acuerdo a las estadísticas, el creciente incremento de los servicios en línea que muchas empresas implementan para mejorar sus servicios también constituye un creciente nivel de riesgos y vulnerabilidad para las mismas. Toda empresa podría ser víctima de ataque informático, sea esta grande, mediana o pequeña, lo que implica una vulnerabilidad en la seguridad de sus datos y riesgos para sus negocios. Actualmente las personas a cargo de la seguridad y la infraestructura de una empresa tienen que lidiar con un sinnúmero de amenazas informáticas, convirtiéndose este en un tema muy apasionante y a la vez complicado. Es por ello que surge la necesidad de implementar un plan preventivo de seguridad que proteja a las empresas de posibles ataques en su red informática.

Existen muchas clases de ataques a sistemas informáticos, como Ataques DoS, ransomware, Ingeniería Social, Phishing, entre otros. Estos buscan aprovechar las debilidades en la red informática de una empresa, atacando distintos puntos, e incluso aprovechando descuidos del personal para infiltrarse en la red y poner en riesgo la seguridad de la empresa.

El presente proyecto contempla una solución tecnológica en la “Fundación para el desarrollo Integral ESPOIR”, que permita la administración de un Sistema de Gestión Unificada de Amenazas UTM. Para este propósito se evaluaron las condiciones iniciales de la empresa en conjunto con el personal de infraestructura. Se desarrolló un conjunto de pruebas de Pentesting, que facilitaron caracterizar las vulnerabilidades existentes en los distintos servicios y sistemas de la institución, y a raíz de estas pruebas, establecer un conjunto de estrategias de seguridad para evitar posibles ataques que puedan poner en riesgo la información de la institución y sus clientes.

ABSTRACT

According to statistics, the growing increase in online services that many companies implement to improve their services also constitutes a growing level of risk and vulnerability to themselves. Every company could be a victim of a computer attack, whether large, medium or small, which implies a vulnerability in the security of its data and risks to the business. Nowadays, people in charge of the security and infrastructure of a company have to deal with countless computer threats, making this a very exciting and complicated issue. That is why arises the importance of implementation of a preventive security plan that protects companies from possible attacks on their computer network.

There are many kinds of attacks on computer systems, such as DoS Attacks, Ransomware, Social Engineering, Phishing, among others. They try to take the advantage of weaknesses in a company's computer network attacking different points, and even taking advantage of staff oversights to infiltrate the network and compromise the security of the company.

This project envisages a technological solution in the "Foundation for Integral Development ESPOIR", which allows the administration of a Unified UTM Threat Management System. The initial conditions of the company were evaluated working with the infrastructure staf. A set of Pentesting tests was developed, which facilitated the characterization of the vulnerabilities existing in the different services and systems of the institution. As result of these tests, were established a set of security strategies to prevent potential attacks that could compromise the information of the institution and its customers.

INTRODUCCIÓN

El presente proyecto técnico es desarrollado con el fin de solucionar de manera óptima los problemas de seguridad de la información existente dentro de la Infraestructura de red de la Fundación para el desarrollo Integral ESPOIR.

Fundación ESPOIR es una entidad financiera que diariamente gestiona un importante flujo de información sensible y confidencial proveniente tanto de sus clientes como de sus procesos administrativos internos; razón por la cual es necesario salvaguardar dicha información de cualquier ataque interno o externo que pueda afectar su integridad y confidencialidad.

Este proyecto se enfoca en una evaluación inicial de las condiciones se vulnerabilidad de la Institución, en conjunto con el personal de infraestructura, con la finalidad de detectar los problemas de seguridad en la red de Fundación ESPOIR, posteriormente se desarrolló un conjunto de pruebas de Pentesting que permitió generar un reporte de vulnerabilidades en los distintos servidores de la institución, y su posterior análisis de riesgo.

Una vez evaluado el riesgo en la red, se analizaron de forma comparativa varias soluciones UTM, que se adapten adecuadamente a las necesidades de la institución, para mitigar las vulnerabilidades que se encontraron en la fase de evaluación.

Finalmente se realizó la instalación y configuración de la Solución UTM más adecuada para la institución, y se realizó el análisis de riesgos residuales posterior a la implementación de la Solución.

CAPÍTULO 1

ANTECEDENTES

1.1 Planteamiento del Problema

La Fundación para el Desarrollo Integral ESPOIR, es una Institución que se dedica a ofrecer microcrédito enfocándose en personal como mujeres de escasos recursos económicos, que residen en áreas urbano-marginales y rurales del país, que tengan o no experiencia en el negocio y que estén interesadas en mejorar sus ingresos y luchar por su bienestar y el de su familia.

La Fundación actualmente dispone de 15 oficinas regionales y la oficina matriz, cada una de las oficinas cuenta con enlaces de datos dedicados en una red MPLS (MultiProtocol Label Switching) del proveedor de servicios Telconet, la red de datos posee una topología en estrella con centro en oficina matriz, donde se encuentran los servidores principales de aplicaciones del negocio, además cada oficina cuenta con su propio Data-Center, con servidores y equipos de red (switches propios y routers del proveedor de enlaces), central telefónica IP conectada a la PSTN (Public Switching Telephone Network).

En la actualidad, ESPOIR gestiona una vasta cantidad de información financiera relacionada principalmente con las transacciones crediticias y comerciales que realizan sus clientes. Considerando que el bien más importante para una organización es la información, su principal objetivo es garantizar la seguridad de los datos de sus clientes y de sus procesos administrativos; no obstante, y debido a la diversificación de sus productos y servicios online, los niveles de riesgo y ataques derivados de las vulnerabilidades se han incrementado notablemente, lo cual podría ocasionar daños e impacto directamente con la integridad, confidencialidad y disponibilidad de la información.

Ante esta realidad, el directorio de ESPOIR ha visto la necesidad de salvaguardar toda la información de sus clientes mediante la implementación de un sistema de Gestión Unificada de Amenazas (UTM).

1.2 Justificación

Considerando que cualquier empresa puede ser víctima de un ataque informático, el presente proyecto es desarrollado con el fin de solucionar de manera óptima los problemas de control de seguridad de la información existente dentro de la Infraestructura de red de datos de Fundación ESPOIR, propios de las actividades de la institución. En muchas circunstancias las actividades de la organización se han visto vulneradas por la falta de un sistema de gestión unificada de amenazas, que pueda gestionar el tráfico de las redes internas de la institución, y permita al profesional encargado del Data Center tener un conjunto de mecanismos y servicios de seguridad para optimizar la administración de los recursos tecnológicos de la organización.

Considerando que ESPOIR es una entidad financiera que día a día tiene un flujo de información confidencial tanto de las socias como del negocio, se busca salvaguardar dicha información de cualquier ataque cibernético que pueda afectar su desarrollo, una de las estrategias para detectar las vulnerabilidades en la infraestructura tecnológica de la institución, es aplicar un conjunto de pruebas de Hacking de manera controlada con el fin de identificar vulnerabilidades en la seguridad y así establecer controles preventivos y correctivos para evitar ataques a los sistemas de la entidad.

Como resultado de estas pruebas, se determinará una línea base en la seguridad con el fin de establecer las herramientas de software o hardware más adecuadas que permitan minimizar las amenazas detectadas para salvaguardar la información, mediante un sistema de gestión de amenazas unificado (UTM), mismo que estará orientado a gestionar la red de amenazas centralizando y simplificando la seguridad y el control de las vulnerabilidades de la red interna de ESPOIR para regular el tráfico defendiendo los intereses y las necesidades de control.

1.3 Objetivos

1.3.1 Objetivo General

Desarrollar un Sistema de Gestión Unificada de Amenazas (UTM) en la Fundación para el Desarrollo Integral ESPOIR que coadyuve a la gestión y protección de la información interna de la organización.

1.3.2 Objetivos Específicos

- Analizar los requerimientos técnicos e institucionales en la infraestructura de red de la fundación para la determinación de una línea base en cuanto a sus problemas de seguridades.
- Definir un conjunto de políticas de seguridad en función de la información recopilada y de las amenazas detectadas.
- Desarrollar una solución integral de seguridad (UTM) para el establecimiento de servicios y mecanismos de protección adecuados para la red de datos aplicando la mejor opción del mercado y que se ajuste a los requerimientos de la empresa.
- Realizar pruebas de hackeo ético para la evaluación de los componentes del UTM seleccionado.

1.4 Marco conceptual

Como parte introductoria, se va a citar la definición de algunos términos que se enmarcan dentro de este proyecto.

- **Activo (Asset):** se define como cualquier sistema, recurso o cosa que tenga un valor para una organización y por lo tanto deba de ser protegida, los Activos pueden ser bienes físicos tales como equipos de cómputo y maquinaria, también puede ser la Información y propiedad intelectual. (Rio, 2017)
- **Adware:** Software publicitario, que tienen algunos programas gratuitos o en fase de prueba que muestran publicidad, mensajes de activación o de compra, comúnmente el creador cobra por la publicidad que se muestra, los mensajes se muestran cuando está en funcionamiento el software asociado. (Rio, 2017)
- **Antivirus:** es un programa informático diseñado para detectar, prevenir y eliminar Software perjudicial o dañino para los sistemas. (Rio, 2017)
- **Análisis de Riesgos:** evaluación sistemática de la información en una red, para identificar peligros y valorar los riesgos. (Poveda, 2011)
- **Amenaza:** Situación con un alto potencial de causar daños, estas pueden ser por robo o divulgación de información, destrucción o alteración de datos o denegación de servicio (DOS). (System, 2016)
- **Negación de servicio (DoS):** Es un ataque a un servicio o sistema que provoca inhabilitar este recurso para los usuarios. (System, 2016)

- **DDoS (Ataque distribuido de negación de Servicios):** Es una clase de ataque distribuido en el que el atacante efectúa ataques simultáneos de negación de servicio a un servidor en una red desde varios sistemas. (Rio, 2017)
- **La confidencialidad:** se define como la necesidad de encubrir cierta información o recurso. Su objetivo principal es, evitar la divulgación no autorizada de información sobre sistemas o recursos de nuestra organización. (ISOToolsExcellence, 2018)
- **La integridad:** La información de una empresa debe mantenerse intacta ante intentos maliciosos que podrían alterar la información sin autorización. Su principal objetivo es prevenir alteraciones en la información que no hayan sido previamente autorizadas. (ISOToolsExcellence, 2018)
- **La disponibilidad:** se refiere a que un sistema informático debe permanecer activo en todo momento sin padecer ninguna degradación. La información siempre deberá mostrarse accesible para usuarios autorizados. Su principal objetivo es evitar las interrupciones de los servicios o recursos informáticos. (ISOToolsExcellence, 2018)
- **Sistema de detección de intrusos (IDS):** se define como el mecanismo de detección de tráfico de la red que de forma discreta descubre actividades sospechosas o anormales con el fin de limitar el riesgo de intrusión. (System, 2016)
- **Sistema de prevención de intrusiones (IPS):** Es el sistema responsable de detectar e impedir la transmisión de código maliciosos, intento de intrusión o cualquier amenaza que pueda atacar nuestra red. (System, 2016)
- **Firewall:** Hace referencia al hardware o programa informático creado para impedir el acceso no autorizado en una red. (System, 2016).
- **Ataque de Fuerza Bruta:** Es una clase de ataque que radica en que el atacante prueba todas las posibles combinaciones de números, letras y caracteres para descifrar la contraseña de un sistema. (Rio, 2017)
- **Vulnerabilidad:** Hace referencia a una deficiencia en la seguridad de una red o servicio o equipo, que es utilizada para acceder a la red y tomar control del equipo completo o de una aplicación. (Esaú, 2018)
- **Exploit:** Es una aplicación programada para explotar las vulnerabilidades de un sistema, de modo que se infiltran en el sistema que contiene la vulnerabilidad para tomar control del mismo o para provocar degradación en su funcionamiento. (Esaú, 2018)

- **Pentesting: l**lamado también “test de penetración” que consta en atacar un sistema informático con la finalidad de descubrir vulnerabilidades y demás errores de seguridad que podrían existir en el sistema y de esta forma crear un plan preventivo de ataques externos. (Esaú, 2018)
- **DMZ:** Proviene de las palabras inglesas “Demilitarized Zone”, que en español significan “Zona desmilitarizada”, que es una red aislada que se encuentra dentro de la red interna de la organización a través de la cual se puede acceder a todos los recursos de la organización, desde Internet, que se encuentra exclusivos en esta red. (Incibe, 2019)
- **UTM:** por sus siglas UTM “(Unified Threat management/Gestión Unificada de Amenazas)” es la nomenclatura dada a un programa informático o dispositivo de hardware que puede agrupar una serie de funciones de seguridad, como proxy, filtro de paquetes, sistemas de detección y prevención de intrusos, control de aplicaciones, entre otros. (Ostec, 2018)
- **Hacker:** se refiere a la persona experta en muchas ramas técnicas relacionadas con las tecnologías de la información y las telecomunicaciones, como hardware de red, sistemas operativos, programación, redes de computadoras, entre otros. (Verdesoto, 2007)
- **Chacker:** Personas que pueden considerarse con un subgrupo secundario de la comunidad de hackers, que se destina a vulnerar la seguridad de un sistema informático, utilizando las mismas herramientas que un hacker pero en diferencia que realiza este ataque con fines explícitos de causar daño o conseguir beneficios personales. El termino Cracker se deriva de la expresión “Criminal Hacker”. (Verdesoto, 2007)

1.4.1 Análisis de Riesgos

(Poveda, 2011) señala: “Dentro del contexto de un análisis de riesgos, es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente”.

Para realizar un análisis de riesgos se procede primero a realizar un inventario de activos Si este inventario es pequeño, puede hacerse el análisis sobre todos los activos que contiene. Si el inventario es extenso, se recomienda seleccionar un grupo manejable o

relevante de activos, sean estos los considerados más estratégicos o los de más valor dependiendo del tipo de evaluación y el análisis del riesgo que se desea aplicar. (Poveda, 2011)

1.4.1.1 Identificar Amenazas

Se puede calificar como amenaza a un incidente o acontecimiento provocado por una entidad que valiéndose de una o varias vulnerabilidades de un activo, pone en peligro la confidencialidad, la integridad o la disponibilidad de este. En resumen, una amenaza aprovecha la vulnerabilidad del activo. Considerando su origen, existen dos tipos de amenazas:

- **Externas:** que son las provocadas por alguien (proveedores, clientes, hackers, etc.) que no pertenece a la organización. Un ejemplo de este tipo de amenazas externas pueden ser los virus o las tormentas
- **Internas:** estas amenazas al contrario son las provocadas por alguien que pertenece a la organización, dentro de estas amenazas pueden ser los errores de usuario o errores de configuración.

Según la intencionalidad del ataque, las amenazas también pueden dividirse en dos grupos: en deliberadas y accidentales:

- **Deliberadas:** estas se catalogan cuando hay una intención de causar un daño, como puede ser un ataque de denegación de servicio o la ingeniería social.
- **Accidentales:** estas se dan cuando no existe la intención de causar daño, como pueden ser averías en los equipos o desastres naturales como incendios, terremotos, inundaciones, etc.

Para evaluar las amenazas en su máximo esplendor se debe considerar cual sería su impacto en caso de que estas amenazas ocurrieran, y cuales serían los parámetros de seguridad como confidencialidad, integridad o disponibilidad, que se verían afectados.. (Poveda, 2011)

1.4.1.2 Identificación de vulnerabilidades

Una vulnerabilidad es toda aquella característica o situación de un activo que facilita un ataque que puede comprometer la confidencialidad, integridad o disponibilidad de este activo. Como ejemplo: un equipo puede llegar a ser vulnerable a un virus si no tiene instalado un programa antivirus. Se debe reconocer las debilidades de una organización

y valorar que tan vulnerable puede llegar a ser un activo en una escala razonable (alto-medio-bajo, de 1 a 5, etc.). Se debe considerar también que por sí misma una vulnerabilidad no produce daño, debería existir una amenaza que explote dicha vulnerabilidad para que esta provoque daño. Algunos ejemplos de vulnerabilidades son:

a) Falta de copias de seguridad, lo que compromete la disponibilidad de los activos.
b) Que los usuarios no tengan conocimiento sobre puntos de vulnerabilidad de la información, siendo los focos de filtrado de información o que cometan errores sin ser conscientes del daño, lo que pone en riesgo la confidencialidad, la integridad y la disponibilidad de los activos.

1.4.2 Hacking Ético

Hacking Ético se define como un conjunto de pruebas de intrusión controladas sobre sistemas informáticos; el consultor o pentester, evalúa una red desde el punto de vista de un cracker, con la intención de encontrar vulnerabilidades que podrían ser explotadas, en los equipos auditados. Estas pruebas de intrusión le permiten al consultor acceder al sistema afectado, siempre en un ambiente controlado o supervisado, para evitar poner en riesgo la operatividad de los servicios de la organización. (Astudillo B., 2018)

1.4.2.1 Fases de Hacking Ético:

Un auditor informático o un cracker, tiene el mismo procedimiento, paso a paso, al momento de efectuar un Pentesting. Esta serie de pasos agrupados se los llama Fases de Pentesting, que constan al menos de los siguientes puntos:

- **Reconocimiento:** Es la recopilación de información acerca de los sistemas de seguridad informática, servicios, programas, protocolos de una organización. También consiste en un análisis técnico con herramientas como Nmap (escaneo de puertos), FOCA (Análisis de metadatos) o PassiveRecon (para Web), entre otras. El reconocimiento de la información o Footprinting, puede ser de dos tipos:
    a. **Reconocimiento activo:** Este tipo de reconocimiento de información se da cuando no tenemos información directa con el cliente o víctima. Ejemplos de reconocimiento activo pueden ser Barridos de Ping, Conexión a un puerto, uso de Ingeniería Social.
    b. **Reconocimiento pasivo:** a diferencia del reconocimiento activo en este tipo de reconocimiento si hay una interacción directa con el objetivo o

víctima. Ejemplos de este reconocimiento pueden ser Búsqueda con Google Hacking Google u Obtención de "vecinos web" de la aplicación.

- **Escaneo:** es la detección de vulnerabilidades en función de la información recopilada en la primera fase del Hacking Ético.
- **Obtener Acceso:** consiste en la explotación de vulnerabilidades halladas y un posterior análisis de la información sobre los posibles efectos causados en el sistema de seguridad o los equipos y los datos sobre el tiempo de respuesta del sistema.
- **Elaboración de Informes:** es la información generada sobre las vulnerabilidades encontradas y como fueron explotadas, acompañado de un análisis del estado del sistema, soluciones a los problemas detectados y recomendaciones. (Andalucia, 2019)

1.4.2.2 Modalidades de Ethical Hacking

Dentro del hacking ético existen diferentes modalidades mismas que se describen a continuación:

- ***Black Box Hacking:*** Este es el denominado "Hacking de caja Negra", en esta modalidad se efectúan pruebas de intrusión externas. Se lo llama así, debido a que el cliente únicamente le otorga al Pentester el nombre de la empresa a ser auditada, de modo que el auditor empieza su trabajo a ciegas, toda la información sobre la organización y su infraestructura es una caja negra para el auditor. Se llama de este modo por que el cliente solamente le proporciona el nombre de la empresa a ser auditada por el consultor, por lo que esté comienza su labor a ciegas, la infraestructura de la organización es una caja negra para él. Este tipo de auditoria es considerada más realista, considerando que el atacante de una organización cuando decide efectuar un ataque, lo único que dispone de información es el nombre de la organización a ataca. Este tipo de ataques al no tener mayor información representa una mayor inversión de tiempo. (Astudillo B., 2018)
- ***Gray Box Hacking:*** A esta modalidad se la denomina "Hacking de Caja Gris". En esta modalidad se efectúa pruebas de intrusión internas. Se la llama Caja Gris al externo cuando el cliente proporciona una limitada información como un listado de datos como el direccionamiento IP o el tipo de función del equipo (router, web service, firewall, entre otros), sobre los equipos a ser auditados de la organización. Se llama Caja Gris al interno cuando el cliente proporciona al

auditor los accesos que tendría un empleado de la empresa como datos de configuración de la red local (dirección IP, mascara de red, Gateway y servidor DNS); pero no le proporciona información como usuarios y claves para acceso al dominio, o información de subredes. (Astudillo B., 2018)

- ***White Box Hacking:*** A esta modalidad se la denomina "Hacking de Caja Blanca", aunque en ocasiones también se le llama hacking transparente. En esta modalidad se aplica a pruebas de intrusión internas solamente y se llama de esta forma por que la empresa cliente le da al consultor la información completa de las redes y los sistemas a ser auditados. Es decir, que además de brindarle un punto de red e información de la configuración, el consultor recibe información extensa como diagramas de red, listado detallado de equipos a auditar incluyendo nombres, tipos, plataformas, servicios principales, direcciones IP, información de subredes, etc. Debido a que el consultor se evita tener que averiguar esta información por sí mismo, este tipo de hacking suele tomar menos tiempo en ejecutarse y por ende reduce los costos de ejecución. (Astudillo B., 2018)

CAPÍTULO 2

EVALUACIÓN INICIAL DE FUNDACIÓN ESPOIR

2.1 Información General

La Fundación ESPOIR inició sus actividades en microfinanzas en enero del 2002, especializándose es el área de crédito grupal (banca comunal) con servicios de educación; su principal objetivo de impulsar el desarrollo económico, social y de salud de microempresarios, en especial de mujeres de sectores vulnerables, que tengan o no experiencia de negocio y que estén determinadas a mejorar sus ingresos, su salud, su capacidad de gestión y a luchar por su bienestar y el de su familia.

"Actualmente Fundación ESPOIR, opera en 6 provincias a nivel nacional: Manabí, El Oro, Guayas, Los Ríos, Santo Domingo de los Tsáchilas y Pichincha. Cuenta con 15 oficinas y 7 puntos de atención. La Fundación tiene presencia en 85 cantones del Ecuador y su oficina Matriz se encuentra en la ciudad de Quito". (ESPOIR, 2018)

2.1.1 Misión

"Impulsar el desarrollo económico, social y de salud de las microempresarias y los microempresarios del Ecuador, con énfasis en la población de menores ingresos; con el propósito de mejorar su calidad de vida y la conservación de su medio ambiente, a través del otorgamiento de servicios microfinancieros y no financieros". (ESPOIR, 2018)

2.1.2 Visión

"Somos una institución de la economía popular y solidaria especializada en microfinanzas, que promueve la inclusión financiera e impulsa el desarrollo y mejoramiento de las condiciones de vida de los microempresarios ecuatorianos, ofreciendo servicios de calidad; lo que nos permite obtener un reconocimiento en el ámbito nacional e internacional. Respaldados por una estructura organizacional competente, comprometida y orientada al cliente". (ESPOIR, 2018)

2.1.3 Ubicación de la oficina Matriz de ESPOIR

La matriz de Fundación ESPOIR se encuentra en la ciudad de Quito D.M. específicamente en la Av. 10 de agosto 5282 y Av. Naciones Unidas, en el edificio Comandato, Torre Iñaquito.

Figura 2.1 Ubicación Oficina Matriz de Fundación ESPOIR

Realizado por: Adriana E. Yánez Tapia

2.2 Levantamiento de Información

Fundación ESPOIR cuenta con una red de datos que interconecta con todas las oficinas de la institución a nivel nacional por medio de enlaces de datos dedicados que confluyen a la oficina matriz, cada enlace de datos es utilizado principalmente para conectarse al sistema principal llamado ORION que se encuentra alojado en el Data-Center ubicado en la oficina matriz, además sirven para dar servicios como acceso a internet, correo electrónico, video conferencias, telefonía IP (Troncales SIP), entre otros.

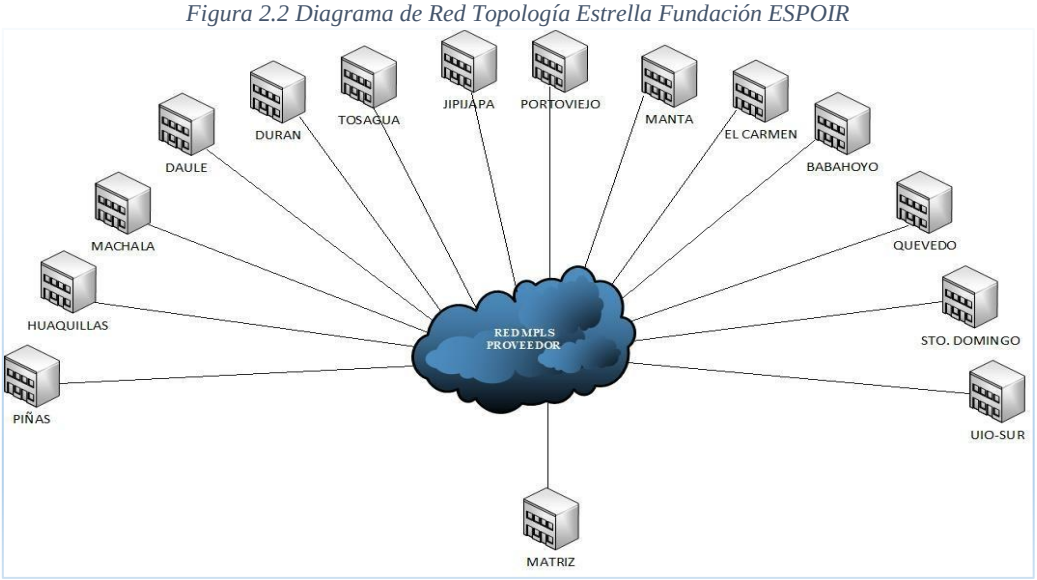
Los enlaces de datos de Fundación ESPOIR se encuentran dentro de la red basada en el protocolo MPLS (Multiprotocol Label Switching) del proveedor de servicios Telconet, estos enlaces de datos son proporcionados a través de fibra óptica, la capacidad de estos enlaces varía de acuerdo al número de usuarios en cada una de las oficinas. Las oficinas cuentan con un ruteador que es administrado por el proveedor de enlaces de datos Telconet.

Cada oficina cuenta con su propia infraestructura local que puede cubrir ciertas necesidades locales para que las oficinas puedan continuar operativas en caso de cortes de enlaces, por ejemplo, las oficinas cuentan con su propio cuarto de servidores, con su servidor local, equipo de comunicaciones, central telefónica IP, AP (Access Point), NAS (Network Attached Storage), equipo UPS (Uninterruptible Power Supply), etc.

2.2.1 Topología Física Actual de la Red de ESPOIR

En la Actualidad, la infraestructura de Fundación ESPOIR cuenta con una topología tipo estrella, dentro de la cual, cada una de sus oficinas a nivel nacional cuenta con enlaces de datos dedicados, dichos enlaces confluyen a su oficina Matriz, dando, de esta manera la forma de una estrella, cada enlace se encuentra en la red MPLS (Multi Protocol Label Switching) de los proveedores de servicios. Cada una de las oficinas, cuentan con dos enlaces configurados como activo-activo los cuales proporcionan redundancia a las comunicaciones, al disponer de un enlace en fibra óptica y un enlace en radio frecuencia por dos diferentes proveedores de servicios de comunicaciones.

Figura 2.2 Diagrama de Red Topología Estrella Fundación ESPOIR



Realizado por: Adriana E. Yánez Tapia

Cada uno de los enlaces de datos cuenta con un AB (ancho de banda) de 4 Mbps y el concentrador de la oficina matriz cuenta con un AB de 56 Mbps. En la Figura 2.2, se puede observar un diagrama de la topología de red estrella de la Fundación ESPOIR.

La red de la oficina matriz de Fundación ESPOIR se basa en una estructura jerárquica de núcleo colapsado, en el cual, las capas de núcleo y la capa de distribución se unifican en una sola capa, a esta capa unificada se conectan los dispositivos de la capa de acceso a la cual se conectan los equipos de usuario final.

La infraestructura cuenta con dos proveedores de servicios de enlaces dedicados, los cuales, acceden a sus equipos en el data center de la institución por medio de fibra óptica, cada proveedor se conecta a un router **Cisco 1811** el cual entrega el acceso a la red MPLS de los enlaces dedicados de las oficinas regionales, el router **Cisco 1811** se conecta al

firewall **Check Point Modelo 5200,** este equipo realiza las funciones de ruteo entre las redes (DMZ, Red Oficina Matriz, Red MPLS de Enlaces dedicados y Salida a Internet).

De una de las interfaces del firewall se conecta al **Swith Aruba 2930F 24G** el cual da acceso a la DMZ (Demilitarized Zone), en este equipo se encuentran configuradas dos VLANs, que se detallan a continuación:

a. **VLAN de Datos:** En esta VLAN se conectan los servidores y dan acceso a los demás equipos del segmento de red, permite a los equipos de usuario final tener acceso a los servicios tales como Core-Bancario, Sistema de Nómina, Aplicaciones de la Institución, Intranet, Web Services, entre otros.
b. **VLAN de Administración:** En esta VLAN se conectan las interfaces de administración ILO de la granja de servidores (Servidores y Storage).

Además, en este segmento de red se cuenta con un Storage, el cual presenta una conectividad a los servidores por Fibra Óptica.

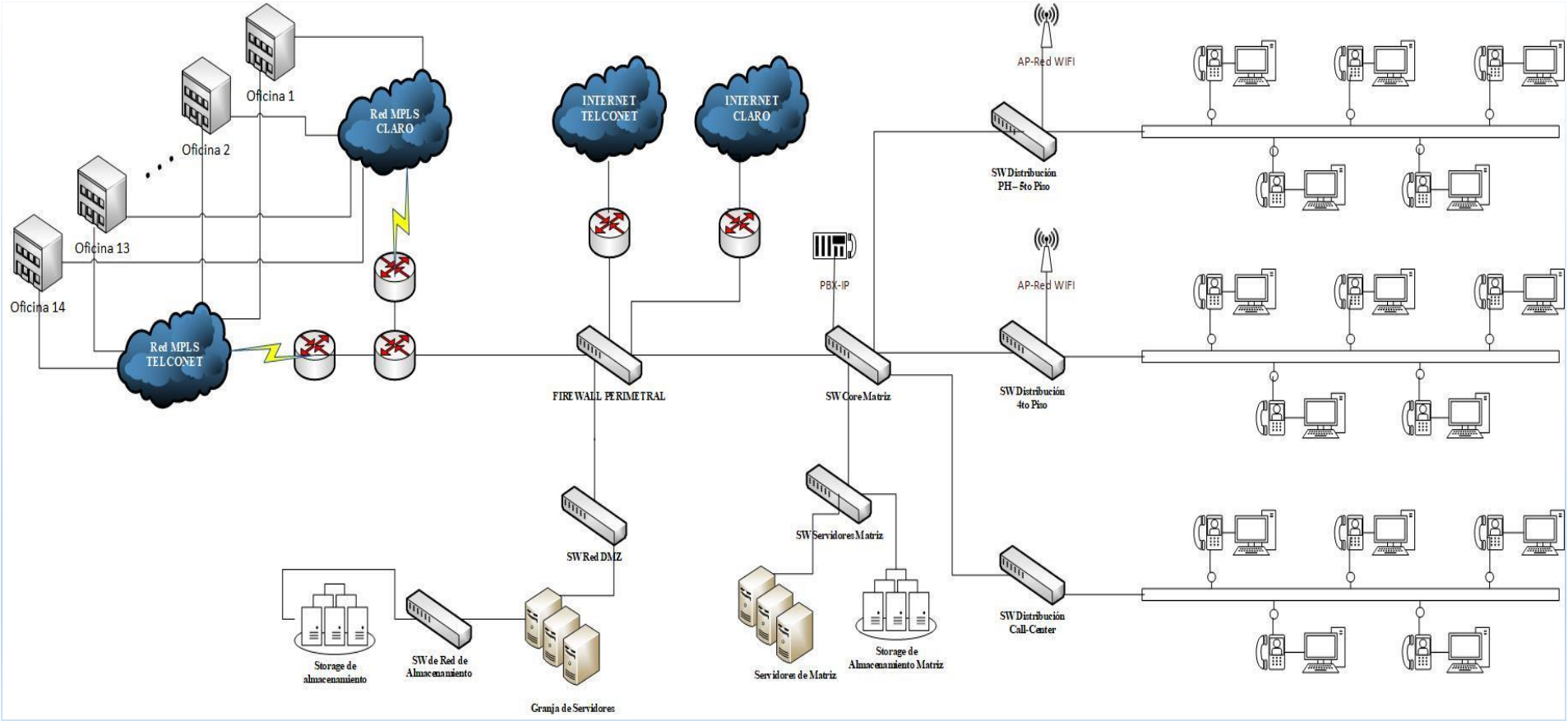
Otra de las interfaces del firewall se conecta al **Switch HPV1910-48G – JE009A** y este a su vez se conecta al **Switch HP 2920-24G - J9726A**, en este Switch se tiene configurado tres VLANs (*Virtual Local Area Network*) para los siguientes servicios:

a. **VLAN de Datos:** Esta VLAN permite a los equipos de la red tener acceso a los servicios tales como FileServers, Active Directory Local, DNS, etc.
b. **VLAN de Almacenamiento:** En esta VLAN se conecta los servidores y Storage, permite el almacenamiento de la información de servidores locales virtualizados.
c. **VLAN de Administración:** En esta VLAN se conectan las interfaces de administración de la granja de servidores (Servidores y Storage).

Adicional, al **Switch HPV1910-48G – JE009A** se conectan tres switches de acceso por medio de enlaces de back-bone, estos switches TPLink Modelo T1600G-52MPS y modelo T2600G-28 MPS, son los encargados de la interconexión de los equipos de usuario final tales como PC (Personal Computer), dispositivos de telefonía IP, dispositivos de impresión, dispositivos de proyección, Access Point y equipos de videoconferencia.

Finalmente, dos interfaces más del equipo firewall se conectan a las salidas a internet de cada uno de los proveedores (Telconet y Claro). En la Figura 2.3, se presenta un mapa de la red correspondiente a oficina Matriz.

Figura 2.3 Diagrama de Red Fundación ESPOIR – Oficina Matriz



Realizado por: Adriana E. Yánez Tapia

2.2.2 Topología Lógica Actual de la Red de ESPOIR / Direccionamiento

El direccionamiento de las redes de Fundación ESPOIR, se encuentra establecido usando protocolo IP versión 4 (IPv4), este tipo de direcciones utiliza la notación decimal/punto para representar cualquier dirección IP.

Cada una de las oficinas de la institución cuenta con su propio segmento de red, el direccionamiento se encuentra establecido con una red privada tipo C, teniendo el siguiente direccionamiento por oficina:

Tabla 2.1 Direccionamiento IP de los Segmentos de Red por Oficina.

REGIONAL	OFICINA	SEGMENTO DE RED	MÁSCARA DE RED	GATEWAY
Pichincha	Matriz	192.168.20.0	255.255.254.0	192.168.20.1
Pichincha	Quito Sur	192.168.14.0	255.255.255.0	192.168.14.1
Sto. Domingo	Sto. Domingo	192.168.11.0	255.255.255.0	192.168.11.1
Los Ríos	Quevedo	192.168.7.0	255.255.255.0	192.168.7.1
Los Ríos	Babahoyo	192.168.8.0	255.255.255.0	192.168.8.1
Manabí	Portoviejo	192.168.1.0	255.255.255.0	192.168.1.1
Manabí	Manta	192.168.2.0	255.255.255.0	192.168.2.1
Manabí	Jipijapa	192.168.3.0	255.255.255.0	192.168.3.1
Manabí	El Carmen	192.168.10.0	255.255.255.0	192.168.10.1
Manabí	Tosagua	192.168.4.0	255.255.255.0	192.168.4.1
Guayas	Durán	192.168.6.0	255.255.255.0	192.168.6.1
Guayas	Daule	192.168.9.0	255.255.255.0	192.168.9.1
El Oro	Machala	192.168.5.0	255.255.255.0	192.168.5.1
El Oro	Piñas	192.168.13.0	255.255.255.0	192.168.13.1
El Oro	Huaquillas	192.168.16.0	255.255.255.0	192.168.16.1

Realizado por: Adriana E. Yánez Tapia

En cada segmento de red se ha realizado una nueva planificación de las direcciones de red con el fin de estandarizar el direccionamiento a nivel nacional, y sea de fácil administración para el encargado de la red, además tratan de respetar el direccionamiento de servicios que se tienen actualmente en ESPOIR.

Tomando en cuenta que cada oficina contará con una red tipo C, y que se disponen de 254 direcciones válidas. En la Tabla 2.2, se presenta el direccionamiento de red usado en los segmentos de red.

Tabla 2.2. Direccionamiento IP de los segmentos de Red

RANGO DE DIRECCIONAMIENTO	USO	DESCRIPCIÓN
1era. Dirección útil	Gateway (Puerta de enlace de red)	Puerta de enlace de red para alcanzar otros segmentos de red.
2da. y 3era. Dirección útil	Servidores de virtualización	Dirección del equipo de virtualización de oficina.
4ta. Dirección útil	Central IP	Dirección de PBX de telefonía IP

6ta. a 15va. Dirección útil	Servidores y Servicios	Servidores Virtuales, Active Directory, Servidor de Aplicaciones, DHCP, FileServer, NAS, etc.
15va. a 19va. Dirección útil	Servicio de Impresiones en Red	Direccionamiento de Impresoras en red.
20va. a 99va. Dirección útil	Rango de equipos de cómputo.	Direccionamiento de equipos de cómputo.
100va. Dirección útil	DVR (Digital Video Recorder)	Dirección de equipo de video DVR
101va. a 159va. Dirección útil	Rango de direcciones de teléfonos IP.	Direccionamiento de teléfonos IP.
160va. a 200va. Dirección útil	Rango de direcciones para equipos portátiles.	Direccionamiento LAN y WLAN para portátiles.
240va. a 254va. Dirección útil	Rango de direcciones de equipos de conectividad.	Direccionamiento de equipos de conectividad switches, Access Point AP y routers.

Realizado por: Adriana E. Yánez Tapia

2.2.3 Equipamiento por Departamentos de Oficina Matriz

La oficina Matriz de Fundación ESPOIR, se encuentra distribuida en dos plantas, dentro de las cuales se subdividen cada uno de los departamentos, en la Tabla 2.3, se presenta el detalle de los departamentos con su ubicación y número de equipos.

Tabla 2.3 Número de equipos por Departamento (PCs, Laptops, Teléfonos IP, Impresoras)

DEPARTAMENTO	UBICACIÓN	# EQUIPOS
Departamento de Tecnología	PH	14
Departamento Financiero	PH	5
Departamento de Contabilidad	PH	7
Dirección Ejecutiva	PH	5
Subdirección Ejecutiva	PH	2
Departamento de Riesgos Financieros	PH	10
Departamento Administrativo	PH	36
Departamento de Talento Humano	4to Piso	10
Departamento de Operaciones	4to Piso	7
Departamento Negocios	4to Piso	8
Departamento de Auditoria Interna	4to Piso	16
Departamento de Salud Ocupacional	4to Piso	3
Departamento de Call-Center	4to Piso	6

Realizado por: Adriana E. Yánez Tapia

2.2.4 Equipamiento de Telecomunicaciones

El equipamiento correspondiente a Telecomunicaciones de Oficina Matriz se describe en la Tabla 2.4.

Tabla 2.4 Equipamiento de Telecomunicaciones Oficina Matriz

TIPO DE EQUIPO	MARCA	MODELO	UBICACIÓN
Servidor	HP	PROLIANT DL-380P GEN-10	Data-Center
Servidor	HP	PROLIANT DL-380P GEN-10	Data-Center
Storage	HP	HPE MSA 2052 SAN SFF STORAGE	Data-Center

Servidor	HP	PROLIANT DL-380P GEN-8	Data-Center
Servidor	HP	PROLIANT DL-360E GEN-8	Data-Center
Servidor	HP	PROLIANT ML-150 GEN-6	Data-Center
Servidor	HP	PROLIANT DL-380 GEN-6	Data-Center
Servidor	HP	PROLIANT DL-380 GEN-7	Data-Center
Storage	HP	STORE VIRTUAL 4330	Data-Center
Storage	HP	STORE VIRTUAL 4330	Data-Center
NAS	D-LINK	DNS-320L	Data-Center
NAS	D-LINK	DNS-320L	Data-Center
Central IP	GrandStream	UCM-6116	Data-Center
DVR	EPCOM	24 CANALES	Data-Center
Firewall	Check Point		Data-Center
Switch	HP	HPV1910-48G – JE009A	Data-Center
Switch	Aruba	ARUBA 2930F 24G 4SFP SWITCH	Data-Center
Switch	HP	HP 2920-24G - J9726A	Data-Center
Switch	TP-LINK	T1600G-52MPS Smart PoE	Data-Center
Switch	TP-LINK	T2600G-28MPS Smart PoE	Rack Auditoria
Switch	TP-LINK	T2600G-28MPS Smart Poe	Rack Call Center
Access Point	Ubikiti	UAP-PRO-3	Administración
Access Point	Ubikiti	UAP-PRO-3	Negocios
Access Point	Ubikiti	UAP-PRO-3	Auditoría Interna
Access Point	Ubikiti	UAP-PRO-3	Sala de Reuniones

Realizado por: Adriana E. Yánez Tapia

2.2.5 Equipamiento Pasivo de Red

Fundación ESPOIR en su oficina matriz se encuentra distribuida en dos (2) pisos, contando con 43 usuarios en oficina, en el piso superior cuenta con su rack de comunicaciones en donde se encuentra el acceso a los proveedores de servicios, el cableado estructurado de éste piso, es de categoría 5e y se distribuye desde el rack de comunicaciones mismo que está alojado en el Data-Center de la oficina, para la planta inferior, esta planta cuenta con dos rack aéreos los cuales dan acceso a las distintas áreas de la oficina. En la Tabla 2.5, se muestra la distribución del equipo pasivo por piso.

Tabla 2.5 Equipamiento pasivo - Ubicación por piso en oficina Matriz

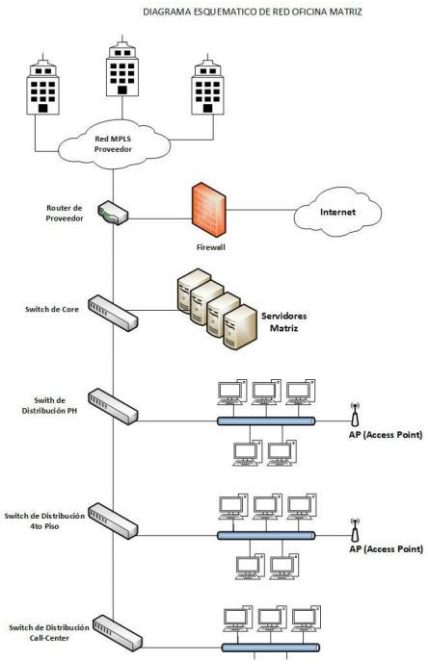
PISO	UBICACIÓN DEL RACK	DEPARTAMENTOS CONECTADOS
PH o 5to. Piso	Data Center en el Departamento de Tecnología.	Dirección Ejecutiva Sub Dirección Ejecutiva Dirección Financiera Administración Dirección de Riesgos Financieros Contabilidad y Tributación Tecnología
4to. Piso	Rack Aéreo en el Departamento de Auditoria	Auditoria Operaciones Negocios Talento Humano Medicina Ocupacional
4to. Piso	Rack Aéreo en el Departamento de	Call- Center

	Call Center	

Realizado por: Adriana E. Yánez Tapia

A continuación, en la Figura 2.4, se muestra el diagrama de Red de equipamiento pasivo de la oficina Matriz, y su distribución por pisos.

Figura 2.4 Diagrama de red de Oficina Matriz – Ubicación por Pisos.



Realizado por: Adriana E. Yánez Tapia

2.2.6 Servicios de Red

Los principales servicios de la Fundación ESPOIR, se encuentran localmente alojados en la siguiente infraestructura:

- **2 servidores HP ProLiant DL380 Gen10,** cada uno con dos procesadores Intel Xeon de la línea Gold modelo 6130 CPU que trabajan a 2.10 GHz, y disponen cada uno de 128 GB de memoria RAM tipo PC4, internamente poseen discos de 300 GB a 15K. Sobre estos discos se encuentra instalado el sistema de virtualización VMware Esxi 6.7, toda esta infraestructura es gestionada por medio de VMware VCenter.
- **Un Storage HPE MSA 2052 SAN DC SFF STORAGE,** el cual dispone de una capacidad de almacenamiento de 12 TB útiles configurado en RAID 5.0 y un almacenamiento all-fash,

Los servidores almacenan bases de datos y otro tipo de información para su consulta por los usuarios de red, los servicios instalados en estos servidores son los siguientes:

a. **Servidor Bases de Datos (SQL Server):** El servidor de Bases de Datos es un servidor virtual con 12 vCPU (Virtual CPU) Intel Xeon 6130 a 2.10 GHz, 40 GB de RAM y un almacenamiento de 700 GB, sobre este equipo se encuentra instalado el sistema operativo Windows Server 2008 R-2 de 64 bits, SQL Server 2008 R-2.
b. **Intranet (WEB Institucional):** El servidor de página web es un servidor virtual con un vCPU (Virtual CPU) Intel Xeon 6130 a 2.10 GHz, 2 GB de RAM y un almacenamiento de 20 GB, sobre este equipo se encuentra instalado el sistema operativo Centos 10, sobre este servidor se encuentra configurado Joomla, para la intranet institucional.
c. **WEB Services:** estos servidores dan acceso a consultas por medio de web services a la base de Datos del Core Financiero.
    - ***Web Services Produbanco:*** El servidor de Web Services es un servidor virtual con 2 vCPU (Virtual CPU) Intel Xeon 6130 a 2.10 GHz, 2 GB de RAM y un almacenamiento de 60 GB, sobre este equipo se encuentra instalado el sistema operativo Windows Server 2003 Standart de 32 bits, en este servidor se encuentra levantado el servicio IIS (Internet Information Services).
    - ***Web Services Equifax:*** El servidor de Web Services es un servidor virtual con 8 vCPU (Virtual CPU) Intel Xeon 6130 a 2.10 GHz, 4 GB de RAM y un almacenamiento de 30 GB, sobre este equipo se encuentra instalado el sistema operativo Windows Server 2012 de 64 bits, en este servidor se encuentra levantado el servicio IIS (Internet Information Services) y SQL Server 2008 Estandar.
d. **Página WEB:** El servidor de página web es un servidor virtual con un vCPU (Virtual CPU) Intel Xeon 6130 a 2.10 GHz, 2 GB de RAM y un almacenamiento de 20 GB, sobre este equipo se encuentra instalado el sistema operativo Centos 10, sobre este servidor se encuentra configurado Joomla, para la página web.
e. **Servidor de Nómina:** El servidor del sistema de Nomina es un servidor virtual que cuenta con 2 vCPU (Virtual CPU) Intel Xeon 6130 a 2.10 GHz, 6 GB de RAM y un almacenamiento de 70 GB, sobre este equipo se encuentra instalado el sistema operativo Windows Server 2008 R-2 de 64 bits, en este servidor se encuentra levantado el servicio de JBoss 7.1 de Java.

f. **Servidor de Aplicación Médica:** El servidor del sistema medico es un servidor virtual que cuenta con 2 vCPU (Virtual CPU) Intel Xeon 6130 a 2.10 GHz, 6 GB de RAM y un almacenamiento de 70 GB, sobre este equipo se encuentra instalado el sistema operativo Windows Server 2008 R-2 de 64 bits, en este servidor se encuentra levantado el servicio de JBoss 7.1 de Java.

g. **Servidor de Replicación**: El servidor del sistema de replicacion es un servidor virtual que cuenta con 8 vCPU (Virtual CPU) Intel Xeon 6130 a 2.10 GHz, 6 GB de RAM y un almacenamiento de 1 TB, sobre este equipo se encuentra instalado el sistema operativo Windows Server 2008 R-2 de 64 bits, para la replicación y respaldo de servidores se encuentra instalado el software Veeam Backup and Replication 10, también el software de replicación requiere de una base de datos en SQL para lo cual se encuentra instalado SQL 2012.

h. **Servidores de Aplicaciones:** Para los servidores de aplicaciones se cuenta con un servidor master y tres servidores esclavos configurados en alta disponibilidad, estos servidores son idénticos y cuentan con las siguientes características, 4 vCPU (Virtual CPU), 4 GB de RAM y un almacenamiento de 40 GB, sobre este equipo se encuentra instalado el sistema operativo Centos 6.7.

2.3 Problemas Detectados

Luego de realizar un análisis completo a la Infraestructura de la Fundación ESPOIR, se detectaron varios problemas con respecto a la seguridad de la red de la Institución, como:

- Los equipos y servicios que forman parte de la infraestructura tecnológica de la Fundación ESPOIR, nunca han tenido una evaluación de seguridad a nivel interno o externo, es decir, nunca se ha realizado una auditoría informática sobre los riesgos de seguridad.
- Durante la evaluación inicial realizada conjuntamente con el personal de infraestructura de la institución, se detectaron varios servicios vulnerables que requieren ser evaluados usando pruebas de pentesting, y a partir del análisis que se ejecutará se aplicará una metodología de hacking de caja blanca o White Box.
- Pese a que la institución cuenta con servicios relacionados a sistemas de seguridad, como un sistema centralizado de gestión de antivirus corporativo “ESET Security Management Center”, para ejecutar políticas de seguridad a los clientes ESET EndPoint Security (Cliente de Usuarios Finales) y ESET File

Security (Cliente de ESET para Servidores), o el sistema de control CheckPoint CloudGuard Saas para la detección y bloqueo de posibles ataques a la plataforma de correo electrónico institucional, no tienen configurados factores de autenticación para ingreso a sesiones de equipos, y además estos sistemas actúan de manera independiente, lo cual provoca que la gestión de seguridad sea dispersa.

- Además de los riesgos asociados a servicios propios de la institución, se detectaron también algunas vulnerabilidades relacionadas con servicios de terceros, como brechas de seguridad en los proveedores en los enlaces.
- También se identificaron riesgos asociados a servicios internos tales como: accesos a las redes inalámbricas, sea para usuarios internos como para usuarios externos o visitantes.
- Cabe tomar en cuenta riesgos asociados a factores totalmente externos como: catástrofes naturales, robo, vandalismo, entre otros.

2.4 Requerimientos

En base a los problemas de seguridad detectados en la Fundación ESPOIR, los requerimientos más importantes para la institución son:

- Realizar pruebas de Pentesting para determinar los riesgos de seguridad describiendo las amenazas y vulnerabilidades en los sistemas y servicios identificados conjuntamente con el personal de la institución, como lo son: Servidor de Base de Datos, Servidor de Aplicaciones, Servidor de Nomina, Servidor de Sistema Medico, Servidor de Intranet, Servidor de página Web, Servidores de Web Services, Servidor de Replicación.
- Realizar un análisis de riesgos para determinar las amenazas existentes, y una vez identificadas dar un tratamiento adecuado para la mitigación o eliminación de las mismas, con el fin de que se garantice un nivel de seguridad adecuado para la institución.
- Evaluar de forma comparativa varias soluciones UTM, que se adapten adecuadamente a las necesidades de la institución, para mitigar las vulnerabilidades que se encontraron en la fase de evaluación.
- Instalar y configurar los módulos de la Solución UTM más adecuada para la institución.

CAPÍTULO 3

PRUEBAS DE PENTESTING

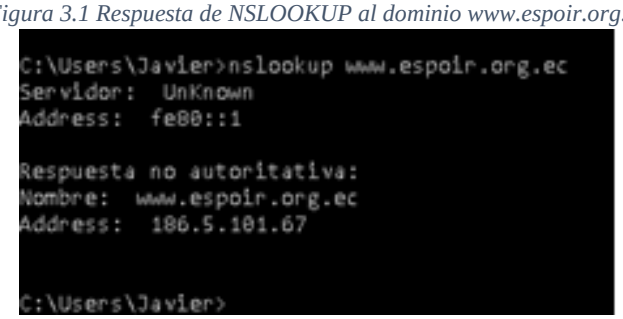
Para el desarrollo del presente proyecto de titulación se realizará un Pentesting a la infraestructura de Fundación ESPOIR, mismo que tendrá una modalidad de White Box Hacking, además el hacking se lo realizará interna y externamente. El proceso constará de tres fases: Reconocimiento, Análisis de Riesgos y Evaluación.

3.1 FASE I: Reconocimiento

3.1.1 Recolección de Información

En esta fase se recolectará la mayor cantidad de información de la Fundación ESPOIR. Para lo cual, se utilizaron varias herramientas, como ***Nslookup***, con la cual se pudo descubrir la dirección IP pública y con la IP publica, se detectó el dominio de la Fundación (www.espoir.org.ec), como se ve en la Figura 3.1.

Figura 3.1 Respuesta de NSLOOKUP al dominio www.espoir.org.ec



Realizado por: Adriana E. Yánez Tapia

Como se observa, la dirección de la IP pública del dominio www.espoir.org.ec, es 186.5.101.67, a partir de ello se verifica la localización geográfica que corresponde a esta IP pública obtenida, para esto se utiliza la búsqueda de la IP en la página www.iplocation.net, obteniendo como resultado: latitud -0,2298 y longitud -78,5250 para la ciudad de Quito a través del proveedor Telconet S.A, la captura de la geolocalización se la puede observar en el Anexo 13.

Además de obtener las posibles coordenadas para la geolocalización de la IP, usando la herramienta ***Whois*** de Kali Linux con el comando ***whois espoir.org.ec >> /home/Adriana /Escritorio/espoir_1.info***, se obtiene información del dominio como fecha de creación, direcciones, entre otros, como se puede ver en el anexo 14, y con el comando DIG se obtuvo información sobre registros NS, SOA y MX del dominio www.espoir.org.ec, en el anexo 15 al 18 podemos ver las respuestas de DIG, en la Tabla 3.1 se muestra un

resumen de la información obtenida del dominio y en la Tabla 3.2, se muestra información de los puertos abiertos.

Tabla 3.1 Información obtenida con la Herramienta Whois

Descripción	Resultado
Dominio	www.espoir.org.ec
Dirección	186.5.101.67
Inetnum	186.5.101.64/24
Status	Real located
Owner	Clientes Quito
Ownerid	EC-CLQUI-LACNIC
Responsable	Tomislav Topic
Address	Kenedy Norte MS-109 Solar 21, 5 Piso
Address	5934 – Guayaquil -Gy
Country	EC
Phone	+593 4 2680555 (101)
Created	2011-08-31
Changed	2018-08-31
espoir.org.ec SOA	Server: ns1.teconet.net e-mail: root@uio.telconet.net
espoir.org.ec A	186.5.101.67
espoir.org.ec MX	Exchange: espoir-org-ec.mail.protection.outlook.com
espoir.org.ec TXT	MS=ms74712688
espoir.org.ec TXT	V=spf1 Include: spf.protection.outlook.com -all
espoir.org.ec NS	ns1.telconet.net ns2.telconet.net ns3.telconet.net
67.101.5.186.in.addr.arpa	PTR mail.espoir.org.ec
101.5.186.in.addr.arpa SOA	Server: ns1.telconet.net Email: abuse@telconet.net
101.5.186.in.addr-arpa NS	ns3.telconet.net ns2.telconet.net ns1.telconet.net

Realizado por: Adriana E. Yánez Tapia

Tabla 3.2 Información sobre puertos abiertos obtenidos con la herramienta Whois

Tipo Puerto	Puerto	Observaciones
FTP	21	220 Bienvenido al Servicio FTP de ESPOIR
SMTP	25	Error TimeOut
HTTP	80	HTTP/1.1 200 OK Server: Apache/2.2.15 (CentOS)

Realizado por: Adriana E. Yánez Tapia

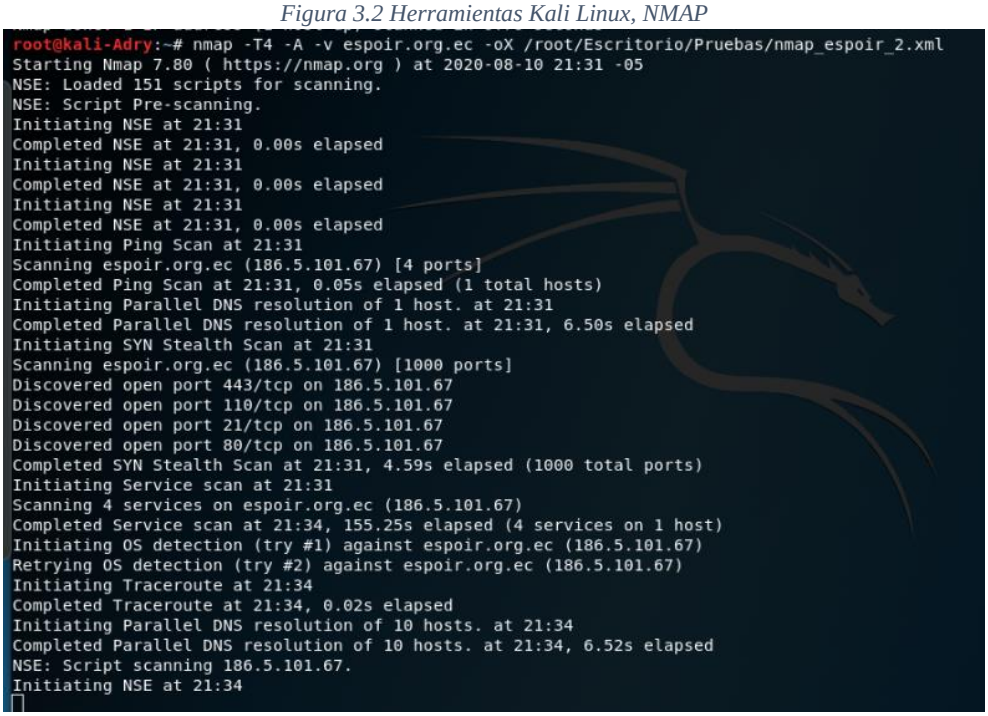
3.1.2 Reconocimiento y Tipificación de Servicios en Fundación ESPOIR.

Considerando que las pruebas de pentesting aplicadas se basan en la modalidad de White Box Hacking, el administrador de la infraestructura ha proporcionado información de los equipos a ser analizados, además de proporcionar un acceso a la red local. Esto sumado

a la información obtenida con la herramienta WHOIS lo cual ayudó con la identificación de los sistemas y servicios.

Usando la herramienta de NMAP se escaneo los equipos para categorizar los servicios existentes en la red, así como, la versión de los sistemas y posibles vulnerabilidades existentes, para lo cual se utilizó el comando **nmap -T4 -A -v IP_Servidor -oX /Destino de la consulta/Nombre_Archivo.xml,** como se observa en la Figura 3.2.

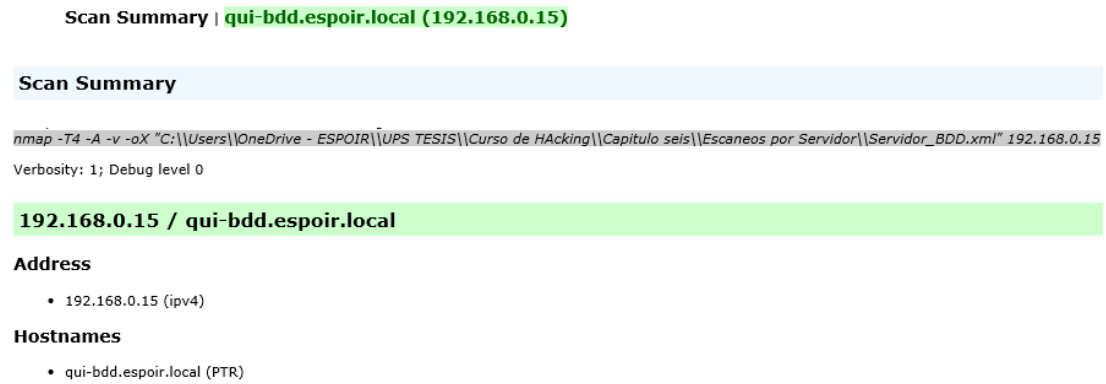
Figura 3.2 Herramientas Kali Linux, NMAP



Realizado por: Adriana E. Yánez Tapia

La ejecución del comando genera un archivo respuesta en formato xml, el cual proporciona la información del equipo escaneado, en la Figura 3.3 se observa el resultado:

Figura 3.3 Resultado del escaneo con NMAP en formato XML del servidor de Base de datos.



Realizado por: Adriana E. Yánez Tapia

La herramienta NMAP**,** proporcionó información muy valiosa y confidencial de la Fundación, lo cual confirmó que le existen brechas de seguridad. Se ejecutó la herramienta NMAP en todos los servidores de la institución, como se ve en las capturas de respuesta en los Anexos 19 a 27. En la Tabla 3.3, se muestra un resumen de los resultados obtenidos:

Tabla 3.3 Resumen de información obtenida con la herramienta NMAP

Resultados de la Herramienta NMAP en los Servidores de ESPOIR				
Servidor	**IP Local**	**Hostname**	**S.O.**	**Servicio**
Servidor de Base de Datos	192.168.0.15	qui-bdd	Microsoft Windows Server 2008 R2 Standard Service Pack 1	Microsoft SQL Server 2008 R2 SP1
Servidor de Aplicaciones	192.168.0.21		Linux 2.6.32	http-server (GlassFish Server Open Source Edition 5.0.1)
Servidor de Nómina	192.168.0.19	qui-n0mina	Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds	Servidor Web: Apache-Coyote/1.1
Servidor de Sistema Medico	192.168.0.18	qui-srvmed	Microsoft Windows Server 2008 R2 Standard Service Pack 1	Http Server (Apache Tomcat 2.4.10)
Servidor de Replicación	192.168.0.197	qui_veeam_srvr	Microsoft Windows Server 2008 R2 Standard Service Pack 1	
Servidor de Intranet	192.168.20.3	intranet	CentOS	Http (Joomla - Apache 2.2.15)
Servidor Web Services Produbanco	192.168.0.204		Microsoft Windows Server 2003 Service Pack 2	Microsoft IIS 6.0
Servidor Web Services Equifax	192.168.0.212	srv-wseqfx	Microsoft Windows Server 2012 R2 DataCenter	Microsoft IIS 8.5
Servidor página Web	192.168.0.2	www.espoir.org.ec	Centos	Http (Apache 2.2.15)

Realizado por: Adriana E. Yánez Tapia

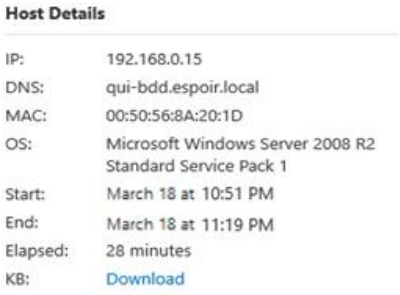
Como resultados de las pruebas realizadas con la herramienta NMAP, se detectaron adicionalmente, varios puertos abiertos como: 21 (FTP), 22 (SSH), 25 (SMTP), 80 (HTTP para servidores Web), 110 (POP3), 135, 139, 445 (Asociados a Netbios), 1720 (Asociado a H323 tipo TCP), 3389 (Microsoft Remote Desktop), 8080 (HTTP para servidores Web Cache).

3.1.3 Análisis de Vulnerabilidades en los Servidores de ESPOIR

Para la revisión de vulnerabilidades de los servidores de Fundación ESPOIR, se utilizó la herramienta Nessus, esta herramienta ayuda a la identificación de vulnerabilidades y problemas de configuración categorizando la información por niveles de severidad, permitiendo un mejor análisis de los riesgos.

En el análisis con Nessus del servidor de Base de Datos, muestra la información como podemos ver en la Figura 3.4:

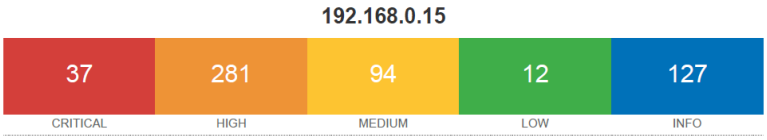
Figura 3.4 Escaneo con la herramienta Nessus del Servidor de Base de Datos.



Realizado por: Adriana E. Yánez Tapia

Con el uso de la herramienta Nessus se puede valorar en base a los colores, el nivel de criticidad de las vulnerabilidades detectadas en el servidor cabe destacar que dichas vulnerabilidades son resultado de un escaneo interno, ya que los servicios de la institución no son publicados al internet a excepción de la página web, en el caso del servidor Web, se hicieron análisis con escaneo interno y externo. En la Figura 3.5, se muestra los resultados obtenidos con la herramienta Nessus, aplicada al Servidor de Base de Datos, el escaneo de todos los servidores se los puede apreciar en los Anexos 28 a 35.

Figura 3.5 Vulnerabilidades encontradas en el Servidor de Base de Datos con Nessus



Realizado por: Adriana E. Yánez Tapia

Terminado el análisis de todos los servidores proporcionados, se ha realizado un cuadro resumen del número de vulnerabilidades encontradas por nivel de criticidad.

Tabla 3.4 Número de Vulnerabilidades encontradas en los Servi dores con Nessus.

	NIVEL DE CRITICIDAD DE VULNERABILIDADES				
Servidor	**# Critical**	**#High**	**#Medium**	**#Low**	**#Info**
Servidor de Base de Datos	37	218	94	12	127
Servidor de Aplicaciones	0	0	1	2	24
Servidor Sistema de Nomina	3	2	10	1	44
Servidor Sistema Medico	12	18	36	1	50
Servidor de Replicación	2	3	13	1	43
Servidor de Intranet	0	0	2	2	29
Servidor Web Services Produbanco	4	3	4	1	36
Servidor Web Services EQUIFAX	0	0	10	1	39
Servidor WEB (Escaneo Externo)	0	0	0	0	6
Servidor WEB (Escaneo Interno)	0	0	3	3	27

Realizado por: Adriana E. Yánez Tapia

3.1.4 Informe del Pentesting

Una vez terminada la fase de reconocimiento, se pudo verificar que el dominio publicado www.espoir.org.ec y la dirección IP pública 186.5.101.67, se evidenciaron los servicios de red TCP, es decir, servicios orientados a la conexión, los mismo que acceden a servicios http (puerto 80), y los demás puertos de este servidor que se muestran expuestos al internet y que han sido obtenidos en el escaneo interno del mismo servidor.

Tabla 3.5 Puertos encontrados en servicios publicados de la Fundación, escaneo externo

Servidor	Puerto	Tipo	Descripción
Servidor Página WEB	21	TCP	Transferencia de Archivos
	80	TCP	Servicio Web
	110	TCP	Recepción de correo electrónico

Realizado por: Adriana E. Yánez Tapia

Para el mismo servidor se realizó un análisis de vulnerabilidades externas, las mismas que no presentan niveles de criticidad crítica o alta, por lo cual en la Tabla 3.6, se presentan los CVE (Common Vulnerabilities and Exposures) de nivel medio y bajo encontrados.

Tabla 3.6 CVE encontrados en servicios publicados de la Fundación, escaneo externo

Servidor	Nivel de Criticidad	CVSS	Descripción de alerta
Servidor Pagina WEB	MEDIUM	5	HTTP TRACE / TRACK Methods Allowed
	MEDIUM	4.3	Apache Server ETag Header Information Disclosure
	MEDIUM	4.3	SSH Weak Algorithms Supported
	LOW	2.6	SMTP Service Cleartext Login Permitted
	LOW	2.6	SSH Server CBC Mode Ciphers Enabled
	LOW	2.6	SSH Weak MAC Algorithms Enabled

Realizado por: Adriana E. Yánez Tapia

Con Nessus se puede presentar un análisis general de las vulnerabilidades CVE internas encontradas, con su respectiva criticidad de los servidores locales, cabe recalcar que en el caso de estos solo se presentan las vulnerabilidades Criticas y Altas, y solo de servidores en la red interna. En la Tabla 3.7, se puede ver este análisis con: Servidor, Nivel de Criticidad, Descripción de la Alerta, Número de Vulnerabilidades asociadas a la descripción.

Tabla 3.7 Número de vulnerabilidades encontradas en los servidores con Nessus

Servidor	Criticidad	Descripción de Alerta	# Asoc	Solución
Servidor de Base de datos	Critica	Security Update	15	Update SO
Servidor de Base de datos	Critica	Could Allow Remote Code Execution	13	Deshabilitar el servicio RDS o permitir el acceso solo desde equipos de confianza
Servidor de Base de datos	Critica	Unsupported Version	5	Ninguna

		Detection		
Servidor de Base de datos	Critica	Uncredentialed check	1	Parchar sistema
Servidor de Base de datos	Critica	Could Allow Elevation of Privilege	3	Parchar sistema
Servidor de Base de datos	Alta	Security Update	141	Update SO
Servidor de Base de datos	Alta	Could Allow Remote Code Execution	71	Deshabilitar el servicio RDS o permitir el acceso solo desde equipos de confianza
Servidor de Base de datos	Alta	Could Allow Elevation of Privilege	53	Parchar SO
Servidor de Base de datos	Alta	Could Allow Denial of Service	16	Parchar SO
Nomina	Critica	Could Allow Remote Code Execution	1	Deshabilitar el servicio RDS o permitir el acceso solo desde equipos de confianza
Nomina	Critica	uncredentialed check	1	Parchar sistema
Nomina	Critica	Unsupported Version Detection	1	Ninguna
Nomina	Alta	Could Allow Remote Code Execution	1	Deshabilitar el servicio RDS o permitir el acceso solo desde equipos de confianza
Nomina	Alta	Security Update	1	Update SO
Replicación	Critica	uncredentialed check	1	Parchar sistema
Replicación	Critica	Unsupported Version Detection	1	Ninguna
Replicación	Alta	Security Update	1	Update SO
Replicación	Alta	SSL Version 2 and 3 Protocol Detection	1	Disable SSL 2.0 and 3.0. Use TLS 1.2
Replicación	Alta	SMBv1 Vulnerabilities	1	Deshabilitar SMBv1 En el servidor
Sistema Medico	Critica	Could Allow Remote Code Execution	1	Deshabilitar el servicio RDS o permitir el acceso solo desde equipos de confianza
Sistema Medico	Critica	uncredentialed check	1	Parchar sistema
Sistema Medico	Critica	OpenSSL 1.0.1	3	Deshabilitar OpenSSL
Sistema Medico	Critica	PHP 5.5.x Multiple Vulnerabilities	6	Upgrade PHP V5.5.32 or Later
Sistema Medico	Critica	Unsupported Version Detection	1	Ninguna
Sistema Medico	Alta	Could Allow Remote Code Execution	1	Deshabilitar el servicio RDS o permitir el acceso solo desde equipos de confianza
Sistema Medico	Alta	Security Update	1	Update SO
Sistema Medico	Alta	Apache 2.2.x Vulnerabilities	2	Upgrade to Apache version 2.2.34 or later.
Sistema Medico	Alta	OpenSSL 1.0.1	1	Deshabilitar OpenSSL
Sistema Medico	Alta	PHP 5.5.x Multiple Vulnerabilities	13	Upgrade PHP V5.5.32 or Later
Web Services Produbanco	Critica	Unsupported Version Detection	3	Ninguna
Web Services Produbanco	Critica	uncredentialed check	1	Parchar sistema
Web Services Produbanco	Alta	Security Update	1	Update SO
Web Services Produbanco	Alta	SMBv1 Vulnerabilities	2	Deshabilitar SMBv1 En el servidor

Realizado por: Adriana E. Yánez Tapia

En el análisis de la red interna de la Fundación, se evidenció los servicios en los servidores, en la Tabla 3.8, se muestra el detalle de los servicios y sus puertos.

Tabla 3.8 Puertos encontrados de servicios de Fundación ESPOIR, escaneo interno.

Servidor	Puerto	Tipo	Servicio	Descripción
Servidor de Base de Datos	25	TCP	Smtp	Transferencia simple de correo
	80	TCP	http	Servicio Web
	110	TCP	pop3	Recepción de correo electrónico
	135	TCP	Msrpc	Gestiona requerimientos Microsoft Remote Procedure Call
	139	TCP	netbios-ssn	Compartimiento de archivos e impresoras en Windows
	445	TCP	microsoft-ds	Compartición de ficheros
	1720	TCP	h323q931	Sirve para proveer paquetes de comunicaciones
	3389	TCP	ms-wbt-server	Remote Desktop Protocol
Servidor de Aplicaciones	22	TCP	Ssh	Secure Shell, para administración remota
	25	TCP	Smtp	Transferencia simple de correo
	80	TCP	http	Servicio Web
	110	TCP	pop3	Recepción de correo electrónico
	1720	TCP	h323q931	Sirve para proveer paquetes de comunicaciones
	3306	TCP	mysql	Puerto de conexión de MySQL
Servidor de Nomina	25	TCP	smtp	Transferencia simple de correo
	110	TCP	pop3	Recepción de correo electrónico
	135	TCP	msrpc	Gestiona requerimientos Microsoft Remote Procedure Call
	445	TCP	microsoft-ds	Compartición de ficheros
	1720	TCP	h323q931	Sirve para proveer paquetes de comunicaciones
	3389	TCP	ms-wbt-server	Remote Desktop Protocol
	8080	TCP	http-proxy	Proxy Http
Servidor de Sistema Medico	25	TCP	smtp	Transferencia simple de correo
	80	TCP	http	Servicio Web
	110	TCP	pop3	Recepción de correo electrónico
	135	TCP	msrpc	Gestiona requerimientos Microsoft Remote Procedure Call
	139	TCP	netbios-ssn	Compartimiento de archivos e impresoras en Windows
	445	TCP	microsoft-ds	Compartición de ficheros
	1720	TCP	h323q931	Sirve para proveer paquetes de comunicaciones
	3306	TCP	mysql	Puerto de conexión de MySQL
	3389	TCP	ms-wbt-server	Remote Desktop Protocol
	8080	TCP	http-proxy	Proxy Http
Servidor de Replicación	25	TCP	smtp	Transferencia simple de correo
	110	TCP	pop3	Recepción de correo electrónico
	111	TCP	rpcbind	Numera solicitudes RPC (Remote Procedure Call)
	135	TCP	msrpc	Gestiona requerimientos Microsoft Remote Procedure Call
	139	TCP	netbios-ssn	Compartimiento de archivos e impresoras en Windows
	445	TCP	microsoft-ds	Compartición de ficheros
	1720	TCP	h323q931	Sirve para proveer paquetes de comunicaciones
	2049	TCP	nfs	Network File System
	3389	TCP	ms-wbt-server	Remote Desktop Protocol
Servidor de Intranet	22	TCP	ssh	Secure Shell, para administración remota
	25	TCP	smtp	Transferencia simple de correo
	80	TCP	http	Servicio Web

	110	TCP	pop3	Recepción de correo electrónico
	1720	TCP	h323q931	Sirve para proveer paquetes de comunicaciones
	3306	TCP	mysql	Puerto de conexión de MySQL
Servidor de Web Services Produbanco	25	TCP	smtp	Transferencia simple de correo
	80	TCP	http	Servicio Web
	110	TCP	pop3	Recepción de correo electrónico
	135	TCP	msrpc	Gestiona requerimientos Microsoft Remote Procedure Call
	139	TCP	netbios-ssn	Compartimiento de archivos e impresoras en Windows
	445	TCP	microsoft-ds	Compartición de ficheros
	1720	TCP	h323q931	Sirve para proveer paquetes de comunicaciones
	3389	TCP	ms-wbt-server	Remote Desktop Protocol
Servidor de Web Services Equifax	25	TCP	smtp	Transferencia simple de correo
	80	TCP	http	Servicio Web
	110	TCP	pop3	Recepción de correo electrónico
	135	TCP	msrpc	Gestiona requerimientos Microsoft Remote Procedure Call
Servidor Pagina WEB	21	TCP	ftp	Transferencia de Archivos
	22	TCP	ssh	Secure Shell, para administración remota
	25	TCP	smtp	Transferencia simple de correo
	80	TCP	http	Servicio Web
	110	TCP	pop3	Recepción de correo electrónico
	1720	TCP	h323q931	Sirve para proveer paquetes de comunicaciones

Realizado por: Adriana E. Yánez Tapia

Como se puede observar en las tablas la mayor parte de servicios no están publicados en el internet, los servicios son internos.

3.2 FASE II: Análisis de Riesgos

Este proceso de Análisis de Riesgos engloba la identificación de los activos informáticos, las vulnerabilidades y amenazas de la institución, además del impacto y la probabilidad de ocurrencia, esto para establecer controles de seguridad adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Los riesgos al estar asociados a la institución fueron considerados en el contexto del giro del negocio y los servicios relacionados al mismo. Por lo cual, se identificaron los activos y se valoró el impacto haciendo relación con el nivel de afectación que puede provocar al negocio.

Dentro de la evaluación del riesgo se debió realizar una valoración del impacto en caso de que el riesgo se presente y una valoración de la probabilidad de la ocurrencia del riesgo, con lo cual se presenta una matriz de riesgos. El riesgo total se determina con la siguiente fórmula:

RT. (riesgo total) = Impacto Promedio ***** Probabilidad

3.2.1 Calificación de Probabilidad e Impacto

Para la calificación de la probabilidad y el impacto se realizaron tablas de ponderación, las cuales, dan calificaciones de acuerdo con el nivel de Criticidad del Incidente y la probabilidad de ocurrencia del incidente.

3.2.1.1 Impacto

Para la realización de la tabla de ponderación del impacto, se analizó el posible impacto que puede provocar a los servicios de la institución y sus afectaciones. En la Tabla 3.9, se presenta las valoraciones.

Tabla 3.9 Calificación de Impacto

IMPACTO			
Tipo	**Calificación**	**Afectación**	**Impacto**
Crítico	5	Pérdida Total del Servicio	Potencialmente irreparable
Alto	4	Pérdida Total del Servicio	Recuperable a mediano plazo
Significativo	3	Degradación o perdida parcial del servicio	Recuperable a Corto Plazo
Moderado	2	Degradación del servicio	Impacto Temporal
Bajo	1	Degradación del servicio	Impacto limitado

Realizado por: Adriana E. Yánez Tapia

3.2.1.2 Probabilidad

Para la realización de la tabla de ponderación de la probabilidad de ocurrencia de impacto, se analizó el posible impacto que puede provocar a los servicios de la institución y sus afectaciones. En la Tabla 3.10, se presenta las valoraciones.

Tabla 3.10 Calificación de Probabilidad

PROBABILIDAD		
Calificación	**Tipo**	**Descripción**
5	Esperado	Alta Probabilidad de convertir las Vulnerabilidades en una amenaza
4	Muy probable	Muy probable de convertir una vulnerabilidad en una amenaza
3	Probable	Probabilidad media de convertir una vulnerabilidad en una amenaza
2	Improbable	Probabilidad baja de convertir una vulnerabilidad en una amenaza
1	Extremadamente improbable	No existe probabilidad de que se pueda convertir una vulnerabilidad en una amenaza.

Realizado por: Adriana E. Yánez Tapia

Para la valoración del impacto y probabilidad de los riesgos tipificados, se consultó a personal del área de infraestructura y aplicaciones de la Institución, los mismos que valoraron los riesgos, cuantificando impacto y probabilidad del evento en la infraestructura actual. De los datos obtenidos se realizó la Tabla 3.11, la misma que muestra los datos y se realiza una cuenta promedio de los datos.

Tabla 3.11 Calificación de Impacto / Probabilidad por el personal del Área de Tecnología.

Amenaza	Tipificación de Riesgo	Impacto /Probabilidad Evaluación N° 1	Impacto /Probabilidad Evaluación N° 2	Impacto /Probabilidad Evaluación N° 3	Impacto /Probabilidad Promedio
SERVIDOR DE BASE DE DATOS	R1	4.9	4.9	4.4	4.73
		1.5	1.7	1.1	1.40
	R2	4.9	4.6	4.2	4.55
		1.1	1.1	1.3	1.17
	R3	4.9	4.9	4.4	4.72
		1.1	1.3	1.2	1.22
	R4	4.9	4.4	4.1	4.46
		1.2	1.4	1.3	1.32
	R5	4.9	4.4	4.6	4.62
		1.1	1.4	1.3	1.27
	R6	4.5	4.6	4.4	4.49
		1.5	1.7	1.9	1.68
	R7	4.5	4.5	4.4	4.47
		1.1	1.4	1.6	1.39
	R8	4.5	4.9	4.7	4.68
		1.1	1.3	1.2	1.21
	R9	4.5	4.4	3.9	4.27
		1.0	1.0	1.0	1.00
NOMINA	R10	3.5	4.2	4.0	3.90
		1.1	1.2	1.2	1.16
	R11	3.3	3.3	3.6	3.41
		1.2	1.2	1.4	1.28
	R12	3.3	3.6	3.5	3.47
		1.1	1.2	1.5	1.27
	R13	3.3	3.6	3.5	3.47
		1.1	1.2	1.5	1.27
	R14	3.3	3.3	3.6	3.41
		1.5	2.0	1.9	1.78
REPLICACIÓN	R15	2.8	2.4	2.6	2.58
		1.2	1.6	1.5	1.43
	R16	2.8	3.1	3.2	3.04
		1.1	1.4	1.3	1.27
	R17	2.5	2.8	2.6	2.63
		1.5	2.0	1.9	1.78
	R18	2.5	2.5	2.8	2.58
		1.1	1.3	1.2	1.21
	R19	2.5	2.8	2.5	2.59
		1.2	1.6	1.4	1.38
SISTEMA MEDICO	R20	2.5	2.8	2.4	2.55
		1.1	1.1	1.2	1.14
	R21	2.2	2.2	2.3	2.24
		1.2	1.6	1.5	1.43
	R22	2.5	2.3	2.7	2.50
		1.5	1.5	1.7	1.55
	R23	2.5	2.8	2.6	2.63
		1.5	1.7	1.6	1.58
	R24	2.5	2.4	2.7	2.51
		1.1	1.3	1.5	1.29
	R25	2.3	2.8	2.6	2.54
		1.1	1.2	1.3	1.19
	R26	2.3	2.5	2.4	2.42
		1.5	1.7	1.7	1.63

	R27	2.3	2.5	2.3	2.39
		1.1	1.4	1.6	1.39
	R28	2.3	2.4	2.3	2.35
		1.1	1.3	1.2	1.21
	R29	2.3	2.3	2.3	2.31
		2.1	1.7	1.5	1.77
WEB SERVICES PRODUBANCO	R30	4.2	4.6	4.3	4.37
		1.1	1.2	1.3	1.19
	R31	4.2	4.4	4.3	4.30
		1.2	1.2	1.4	1.28
	R32	4.0	4.0	4.0	4.00
		1.5	2.0	1.9	1.78
	R33	4.0	4.0	4.2	4.07
		1.2	1.2	1.2	1.20
Catástrofes Naturales	R34	4.9	4.4	4.4	4.56
		0.5	0.7	0.6	0.59
Vandalismo/Robo	R35	4.8	4.8	4.8	4.79
		0.5	0.7	0.6	0.58
Cortes de Servicios de enlaces	R36	4.9	4.9	4.4	4.72
		1.5	1.7	1.5	1.55
Cortes de energía eléctrica	R37	3.0	3.6	3.0	3.19
		1.5	1.5	1.6	1.53
WIFI	R38	2.0	2.6	2.5	2.38
		2.0	2.4	2.2	2.20
Usuarios Externos	R39	1.5	1.8	1.8	1.71
		1.5	2.0	1.9	1.78

Realizado por: Adriana E. Yánez Tapia

3.2.2 Matriz y Mapeo de Riesgos

Se efectuó un análisis general de los riesgos presentes en la red de la Fundación ESPOIR, determinando las amenazas que se hallaron en los equipos especificados por el administrador de la red y otros factores que generan riesgos adyacentes tales como: Catástrofes naturales, vandalismo y robo, cortes de enlaces, cortes de energía eléctrica, WIFI y usuarios externos. A estos también se les asignó una calificación:

Tabla 3.12 Matriz de Riesgos – Calificación promedio de Impacto y Probabilidad

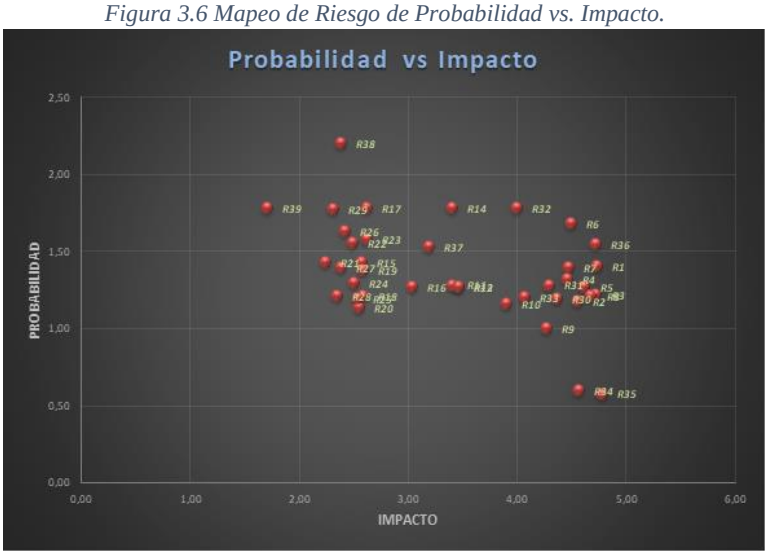
Servidor	Nivel de Criticidad	Descripción de Alerta	Etiqueta	Impacto	Probabilidad
Servidor de Base de datos	Critica	Security Update	R1	4.73	1.40
Servidor de Base de datos	Critica	Could Allow Remote Code Execution	R2	4.55	1.17
Servidor de Base de datos	Critica	Unsupported Version Detection	R3	4.72	1.22
Servidor de Base de datos	Critica	uncredentialed check	R4	4.46	1.32
Servidor de Base de datos	Critica	Could Allow Elevation ofPrivilege	R5	4.62	1.27
Servidor de Base de datos	Alta	Security Update	R6	4.49	1.68
Servidor de Base de datos	Alta	Could Allow Remote Code Execution	R7	4.47	1.39
Servidor de Base de datos	Alta	Could Allow Elevation ofPrivilege	R8	4.68	1.21
Servidor de Base de datos	Alta	Could Allow Denial of Service	R9	4.27	1.00
Nomina	Critica	Could Allow Remote Code Execution	R10	3.90	1.16

Nomina	Critica	uncredentialed check	R11	3.41	1.28
Nomina	Critica	Unsupported Version Detection	R12	3.47	1.27
Nomina	Alta	Could Allow Remote Code Execution	R13	3.47	1.27
Nomina	Alta	Security Update	R14	3.41	1.78
Replicación	Critica	uncredentialed check	R15	2.58	1.43
Replicación	Critica	Unsupported Version Detection	R16	3.04	1.27
Replicación	Alta	Security Update	R17	2.63	1.78
Replicación	Alta	SSL Version 2 and 3 Protocol Detection	R18	2.58	1.21
Replicación	Alta	SMBv1 Vulnerabilities	R19	2.59	1.38
Sistema Medico	Critica	Could Allow Remote Code Execution	R20	2.55	1.14
Sistema Medico	Critica	uncredentialed check	R21	2.24	1.43
Sistema Medico	Critica	OpenSSL 1.0.1	R22	2.50	1.55
Sistema Medico	Critica	PHP 5.5.x Multiple Vulnerabilities	R23	2.63	1.58
Sistema Medico	Critica	Unsupported Version Detection	R24	2.51	1.29
Sistema Medico	Alta	Security Update	R26	2.42	1.63
Sistema Medico	Alta	Apache 2.2.x Vulnerabilities	R27	2.39	1.39
Sistema Medico	Alta	OpenSSL 1.0.1	R28	2.35	1.21
Sistema Medico	Alta	PHP 5.5.x Multiple Vulnerabilities	R29	2.31	1.77
Web Services Produbanco	Critica	Unsupported Version Detection	R30	4.37	1.19
Web Services Produbanco	Critica	uncredentialed check	R31	4.30	1.28
Web Services Produbanco	Alta	Security Update	R32	4.00	1.78
Web Services Produbanco	Alta	SMBv1 Vulnerabilities	R33	4.07	1.20
Catastrofes Naturales			R34	4.56	0.59
Vandalismo/Robo			R35	4.79	0.58
Costes de Servicios de enlaces			R36	4.72	1.55
Cortes de energia electrica			R37	3.19	1.53
WIFI			R38	2.38	2.20
Usuarios Externos			R39	1.71	1.78

Realizado por: Adriana E. Yánez Tapia

Para poder observar la distribución del Riesgo Total que es igual al producto del impacto por la probabilidad de ocurrencia se realizó un diagrama de Probabilidad vs. Impacto

Figura 3.6 Mapeo de Riesgo de Probabilidad vs. Impacto.



Realizado por: Adriana E. Yánez Tapia

3.3 FASE III: Fase de Evaluación

En la fase de evaluación se analizó las opciones que se tienen en el mercado para UTM, características principales, costos, posicionamiento en el cuadrante de Gartner, entre otros

3.3.1 Cuadrante Mágico de Gartner

El cuadrante mágico de Gartner nos sirve como referencia para la posible selección de un UTM, ya que presenta las alternativas que lideran el mercado. Como se puede observar en la Figura 3.7, se proporciona información al año 2019 que es la más actual para UTM siendo Palo Alto Neworks y Fortinet los fabricantes líderes.

Figura 3.7 Cuadrante Mágico de Garner para soluciones UTM al 2019

Realizado por: Adriana E. Yánez Tapia

3.3.2 Opciones de Soluciones UTM en el Mercado

Revisando la información de distintas fuentes acerca de UTM Open Source, se encuentra que la solución más confiable y aceptada es la de PFSense seguida en la mayoría de las oportunidades de OPNSense, por lo cual se evaluará esta opción dentro de las posibles alternativas de implementación.

Además, en la página de IT Central Station, que evalúa a todas las opciones de Firewalls de manera general ubica a PFSense como una de las principales alternativas. En el Anexo 36, se puede observar el ranking, que lo coloca en la posición número 2 solo por debajo de Fortinet.

3.3.3 Análisis Técnico de las Soluciones UTM

Una vez seleccionadas las alternativas de UTM que se podrían implementar de acuerdo con las referencias revisadas del cuadrante mágico de Gartner y las opciones de UTM de software libre; se configuró una tabla comparativa de las características de las siguientes alternativas: Fortinet y Palo Alto (Referencia Cuadrante Mágico de Garther), Fortinet y PFSense (IT Central Station y Redes Zone Net) y Check Point.

En la Tabla 3.13, se muestran de forma comparativa las principales características de los diferentes UTM analizados que actualmente se ofrecen en el mercado:

Tabla 3.13 Comparativa de Características UTM.

	Características	Check Point	PFsense	Fortinet	Palo Alto
Administración e Implementación	Administración WEB	✓	✓	✓	✓
	Administración a través de cliente	✓	×	✓	✓
	Appliance Físico	✓	×	✓	✓
	Implementación en entorno Virtual	✓	✓	✓	✓
Funcionalidades	Firewall	✓	✓	✓	✓
	VPN	✓	✓	✓	✓
	IPS	✓	✓	✓	✓
	IDS	✓	✓	✓	✓
	Control de Aplicaciones	✓	✓	✓	✓
	URL Filtering	✓	✓	✓	✓
	Filtrado de Contenidos	✓	✓	✓	✓
	Anti-Bot	✓	✓	✓	✓
	Anti-Virus	✓	✓	✓	✓
	Anti-Spam	✓	✓	✓	✓
	SandBox	✓	×	✓	✓
	Traffic Shaping	✓	✓	✓	✓
	DLP (Data Lost Prevention)	✓	✓	✓	✓
Otros	Configuración en HA (High Availability)	✓	✓	✓	✓
	Backup y Restauración	✓	✓	✓	✓
	Actualizaciones	✓	✓	✓	✓
	Generacion de reportes	✓	✓	✓	✓
	Costo de Licencia	✓	×	✓	✓
	Otros costos relacionados	✓	×	✓	✓

Realizado por: Adriana E. Yánez Tapia

Como se puede observar, pese a que PFSense no requiere la adquisición necesaria de un equipo en específico, ofrece la opción de una appliance físico, precargada con la configuración base del UTM, pero en caso de no requerirlo se lo puede implementar de manera virtual en algún equipo existente en la infraestructura actual, tomando en cuenta que este no requiere licenciamiento para su implementación, y no requiere la incurrencia en gastos adicionales como costo de renovación de licencias o mantenimiento anual, como ocurre en las otras alternativas presentes en la tabla comparativa.

3.3.4 Consideraciones Técnicas para la Implementación del PFsense

Para la implementación del UTM con PFSense se tomaron en cuenta los siguientes factores:

- Rendimiento requerido: Throughput
- Características o paquetes adicionales de PFSense a ser usados

Estos dos factores van a influenciar en las capacidades a tomar en cuenta en características como RAM, CPU y almacenamiento.

3.3.5 Rendimiento requerido (Throughput)

Por definición Throughput, es la capacidad de transmisión efectiva, por lo que es importante determinar el mismo en la red antes de instalar la solución, porque esto determina el tipo de CPU a utilizar. Si es necesario menos de 10Mbps, entonces es posible utilizar los requerimientos mínimos para el hardware.

- CPU: Cualquier CPU con al menos 100MHz
- RAM: 128 Mb
- Disco: 1 GB

Pero para Throughput superiores se tiene como referencia la Tabla 3.14, en la cual se indica el tipo de CPU base requerido para la implementación, obtenido de la página http://www.firewallhardware.es/medir_hardware_pfsense.html

Tabla 3.14 Requisitos de CPU con Throughput entre 1 a más de 750

Throughput: Mbps	Requisitos de CPU
1-10 Mbps	No menos de 500 MHz CPU Single Core
11-150 Mbps	No menos de 1000 MHz CPU Single Core
51-350 Mbps	No menos de 1.4 GHz CPU Single/Dual Core
100-750 Mbps	No menos de 1.8 GHz CPU Dual Core
750 + Mbps	No menos de 1,8 GHz Dual Core. NIC Intel

Realizado por: Adriana E. Yánez Tapia

3.3.6 Paquetes adicionales

Se debe tener en cuenta los paquetes que se desea implementar de manera adicional a los que por defecto vienen en la instalación base. Pero no se ha planteado la implementación de características adicionales en nuestra implementación, por lo cual el factor de paquetes adicionales no afectaría en el dimensionamiento de la solución. De acuerdo con los requerimientos, se dimensiona para los siguientes parámetros que se muestran en la Tabla 3.15.

Tabla 3.15 Requerimientos de Base para implementación.

Rendimiento de la Solución	
Parámetros Recomendados	
Throughput	500 Mbps
Sesiones concurrentes	125 K

Realizado por: Adriana E. Yánez Tapia

Conforme a los requerimientos base, se procede a analizar la recomendación para la implementación y se parametriza la creación del equipo virtual a ser usado para la implementación considerando el equipamiento disponible en la infraestructura actual de la institución, esto datos se presentan en la Tabla 3.16.

Tabla 3.16 Características de Implementación para PFSense en nuestro habiente virtual

	Recomendación	**Implementación**
Tipo de Implementación	Virtual	Virtual
Procesamiento	Procesador de al menos 1.8 GHz y al menos Dual Core	Procesador Intel Xeon X5690 a 3.47 GHz
RAM	512MGB	4 GB
Almacenamiento	1 GB	100 GB

Realizado por: Adriana E. Yánez Tapia

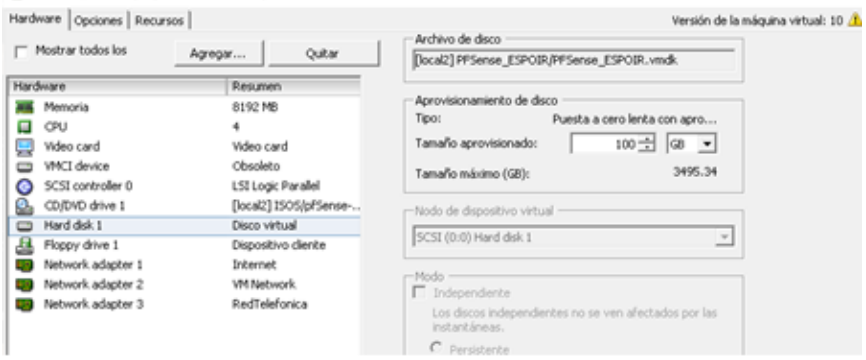
CAPÍTULO 4

IMPLEMENTACIÓN DE SOLUCIÓN UTM

4.1 Instalación de la Solución

Para la implementación de la solución se procedió con la creación de una máquina virtual, se colocaron tres interfaces de red, almacenamiento de 100 GB en el storage local del servidor, Sistema Operativo (FreeBSD 64 Bits), memoria RAM de 8 GB y 4 vCPU.

Figura 4.1 Características de la máquina virtual

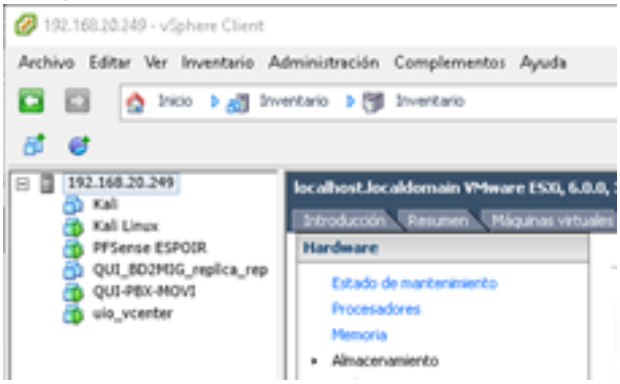


Realizado por: Adriana E. Yánez Tapia

4.1.1 Instalación y Configuración inicial de PFSense

Para instalar el software de PFSense iniciamos la VM (Virtual Machine) PFSense ESPOIR, una vez iniciada la máquina vamos a proceder con la instalación del software necesario.

Figura 4.2 Panel de Administración de VM de VMware



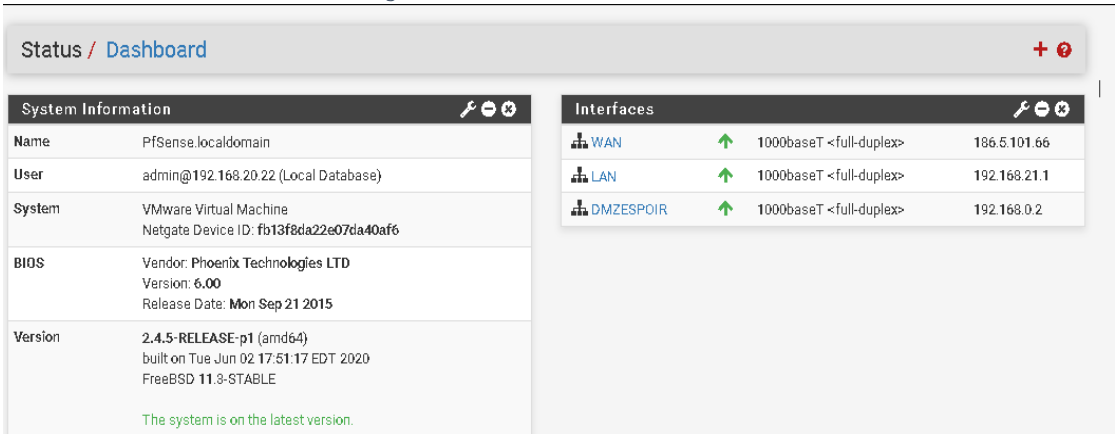
Realizado por: Adriana E. Yánez Tapia

Una vez iniciada la instalación, se aceptó la licencia del producto, se asignó los parámetros de configuración, se reinició la VM, y se inicializó la Aplicación. Se ingresa por medio de un navegador web a la interfaz configurada dentro de la red LAN. Dentro de las configuraciones iniciales se configura el hostname, los DNS, el servidor de NTP, usando los valores por defecto para la configuración inicial.

4.1.2 Configuración de Interfaces

Finalmente se configuran las interfaces de red, las cuales se utilizarán en la configuración inicial para definir interfaces WAN y LAN. En la Figura 4.2, se muestra el Panel de Control de la Aplicación con las interfaces configuradas:

Figura 4.3 Panel de estado del PFSense



Realizado por: Adriana E. Yánez Tapia

4.2 Configuración de PFSense

Para la configuración del firewall se definieron algunos parámetros como reglas de NAT, Alias de Equipos, redes y Servicios, Reglas en las interfaces. A continuación, se presenta algunas de estas configuraciones:

4.2.1 Configuración de ALIAS.

Se definieron alias en la configuración de PFSense para grupos de direcciones IP como servidores de impresión, equipos AP, Servidores AD (Active Directory), direcciones IP de Servidores, segmentos de red de oficinas.

Estos alias tienen la finalidad de ahorrar escritura en las reglas de firewall (en lugar de definir una regla por un objeto se define por un grupo, el cual está definido en el alias previamente configurado). Además, permite realizar cambios en la configuración de una manera más sencilla y rápida, al actuar como parámetros. En el Anexo 37, se observa la definición del alias de red para las redes de las oficinas sucursales, en este proceso se define todas las redes LAN de las sucursales.

Así como se definió las redes locales, también se procedió a la creación de alias para los servidores como servidor web, servidor de nómina, servidor de sistema médico, etc. Una vez definidos todos los alias que se requirieron, se tiene el siguiente resultado, en la Figura 4.4, se observa los alias definidos dentro del PFSense.

Figura 4.4 Resumen de los Alias definidos en PFSense.

Firewall Aliases IP

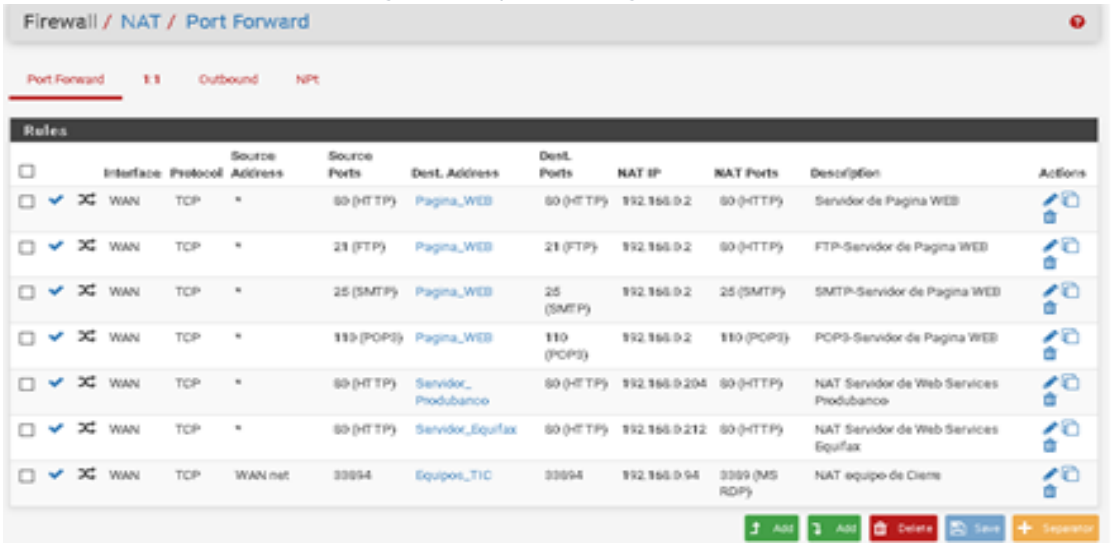
Name	Values
AP_Ubiquiti	192.168.21.240, 192.168.21.241, 192.168.21.242, 192.168.21.243, 192.168.21.244
Area_Contable	192.168.20.31, 192.168.20.32, 192.168.20.33
Base_Datos	192.168.0.15
Centrales_IP	192.168.20.152, 192.168.1.4, 192.168.2.4, 192.168.3.4, 192.168.4.4, 192.168.5.4, 192.168.6.4, 192.168.7.4, 192.168.8.4, 192.168.9.4...
DVR_Matriz	192.168.20.103
Equipos_Administracion	192.168.20.90, 192.168.20.91, 192.168.20.92
Equipos_Coordinadores	192.168.14.20, 192.168.7.20, 192.168.8.20, 192.168.11.20, 192.168.1.22, 192.168.2.23, 192.168.3.19, 192.168.4.20, 192.168.6.21, 192.168.9.20...
Equipos_Directores	192.168.20.30, 192.168.20.20, 192.168.20.70, 192168.20.60, 192.168.20.68, 192.168.20.73, 192.168.20.66, 192.168.20.41
Equipos_Impresoras	192168.20.230, 192.168.20.231, 192.168.20.232, 192.168.20.233, 192.168.20.234, 192.168.20.235
Equipos_Oficiales_Nacionales	192.168.20.80, 192.168.20.81, 192.168.20.82, 192.168.20.83, 192.168.20.86, 192.168.20.87, 192.168.20.88, 192.168.20.89
Equipos_TIC	192.168.20.21, 192.168.20.22, 192.168.20.23, 192.168.20.24, 192.168.20.25, 192.168.20.26, 192.168.20.27, 192.168.20.28, 192.168.20.29
Pagina_WEB	192.168.0.2
Red_Matriz	192.168.20.1/23

Realizado por: Adriana E. Yánez Tapia

4.2.2 Configuración de Reglas NAT (Network Address Translation)

En la configuración se definieron reglas de ruteo para los servicios publicados, por medio del NAT se redireccionan los requerimientos externos a las direcciones IP privadas que atienden el requerimiento. En la Figura 4.5, se observa el resumen de las reglas de redirección del NAT configuradas en el PFSense.

Figura 4.5 Definición de reglas de NAT



Realizado por: Adriana E. Yánez Tapia

4.2.3 Configuración de políticas de seguridad

En las reglas creadas para la aplicación de PFSense de Fundación ESPOIR, se definen el control de tráfico entrante y saliente en la red. Se han definido algunas reglas en las diferentes interfaces que se configuraron en la aplicación teniendo reglas en la LAN, DMZ y WAN.

4.2.3.1 Configuración de políticas de seguridad / LAN

En las reglas de tráfico entrante y saliente de la interfaz LAN, se configuró inicialmente la regla Anti-Lookout Roule o regla de antibloqueo la cual permite tener acceso a la GUI de PFSense y posteriormente definieron las reglas de acceso a redes y servicios como: redes LAN de oficinas sucursales, servicios como páginas Web, servidor de base de datos, servidor de nómina y demás servicios de la red. En la Figura 4.6, se observan las reglas definidas en la interfaz LAN.

Figura 4.6 Definición de reglas de navegación interfaz LAN

Rules (Drag to Change Order)

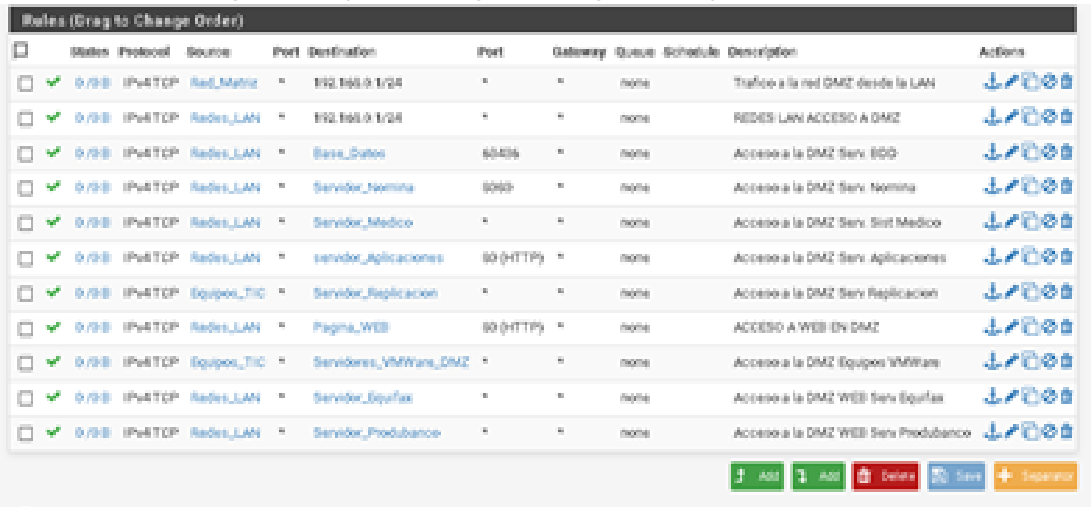
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	1 /5.74 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙
☐ ✓	0 /0 B	IPv4 TCP	*	*	Redes_LAN	*	*	none		Trafico redes LAN	⚓ ✎ ⧉ ⊘ 🗑
☐ ✓	0 /0 B	IPv4 TCP	Redes_LAN	*	Base_Datos	63436	*	none		Conexion a BDD	⚓ ✎ ⧉ ⊘ 🗑
☐ ✓	0 /0 B	IPv4 TCP	Redes_LAN	*	Servidor_Nomina	*	*	none		Servidor de Sistema de Nomina	⚓ ✎ ⧉ ⊘ 🗑
☐ ✓	0 /0 B	IPv4 TCP	Redes_LAN	*	servidor_ Aplicaciones	*	*	none		Servidor de aplicaciones internas	⚓ ✎ ⧉ ⊘ 🗑
☐ ✓	0 /0 B	IPv4 TCP	Redes_LAN	*	Servidor_Medico	*	*	none		Servidor de Aplicacion Sistema Medico	⚓ ✎ ⧉ ⊘ 🗑
☐ ✓	0 /0 B	IPv4 TCP	Equipos_TIC	*	Servidor_ Replicacion	*	*	none		Acceso a servidor replicaicon	⚓ ✎ ⧉ ⊘ 🗑
☐ ✓	0 /0 B	IPv4 TCP	Redes_LAN	*	Servidor_Equifax	*	*	none		Acceso a Equifax	⚓ ✎ ⧉ ⊘ 🗑
☐ ✓	0 /0 B	IPv4 TCP	Redes_LAN	*	Servidor_ Produbanco	*	*	none		Servidor de Web Services Produbanco	⚓ ✎ ⧉ ⊘ 🗑
☐ ✓	0 /0 B	IPv4 TCP	Redes_LAN	*	Servidor_Intranet	*	*	none		Acceso a Servidor de Intranet	⚓ ✎ ⧉ ⊘ 🗑

Realizado por: Adriana E. Yánez Tapia

4.2.3.2 Configuración de políticas de seguridad / DMZ ESPOIR

En las reglas de tráfico entrante y saliente de la interfaz DMZ ESPOIR, se definieron igualmente reglas de acceso a servicios de la red, tomando en cuenta que los servicios de los servidores están en este segmento de red. En la Figura 4.7, se observan las reglas definidas en la interfaz DMZ ESPOIR.

Figura 4.7 Definición de reglas de navegación interfaz DMZ ESPOIR

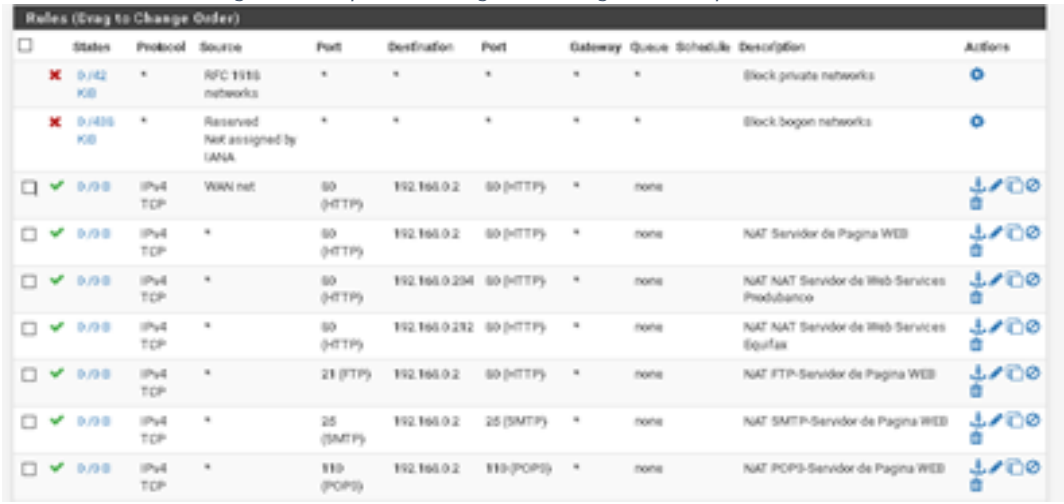


Realizado por: Adriana E. Yánez Tapia

4.2.3.3 Configuración de políticas de seguridad/WAN

Finalmente, en la Figura 4.8, se puede observar las políticas de navegación creadas para la interfaz WAN, mismas que permiten el paso a servicios publicados como: HTTP, FTP; SMTP, entre otros.

Figura 4.8 Definición de reglas de navegación interfaz WAN



Realizado por: Adriana E. Yánez Tapia

4.3 Pruebas de Pentesting posterior a la Implementación

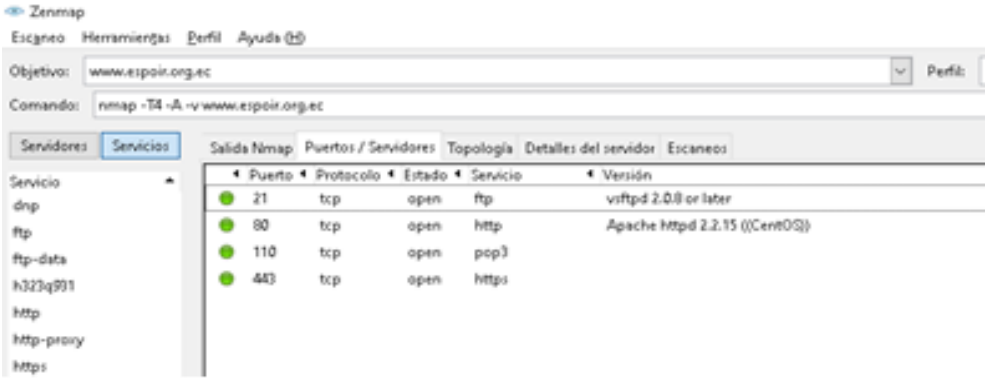
En esta etapa, se revisaron nuevamente las vulnerabilidades de la red después de aplicada la configuración de UTM, hay que recordar que la suma de las vulnerabilidades encontradas consiste en el uso de las aplicaciones que se corren en los servidores que tiene contacto con internet y los puertos abiertos, además de otros factores propios como ex–funcionarios que pudieran intentar atentar contra la institución.

Debido a esto, el Pentesting, se lo realizará en dos etapas: Identificación de sistemas servicios y análisis de vulnerabilidades posteriores a la implementación.

4.3.1 Identificación de Sistemas y Servicios posterior a la implementación

Utilizando la herramienta ZENMAP, se escaneó los equipos de servicios existentes en la red, de esta manera obtenemos información nuevamente de versión de sistemas, puertos abiertos, entre otros; para identificar las vulnerabilidades existentes posterior a la implementación de la Solución PFSense, para este proceso se utilizó el comando: **"nmap -T4 -A -v IP_Address_Servidor".** La ventaja de esta herramienta, que nos permite ver en la pestaña "puertos" un resumen de los puertos encontrados, como se muestra en la Figura 4.9.

Figura 4.9 Escaneo con la herramienta ZENMAP al servidor WEB (Puertos / Servicios)



Realizado por: Adriana E. Yánez Tapia

En la Figura 4.10, se muestra la respuesta de la herramienta ZENMAP aplicada al servidor Web, proporcionándonos la siguiente información: **Servidor:** Servidor Web, **Hostname:** www.espoir.org.ec, **IP Pública:** 186.5.101.67, **IP Local:** 192.168.0.2, **Servicio:** Http (Apache 2.2.15), **SO:** Centos.

Figura 4.10 Información obtenida del Servidor de WEB con la herramienta ZENMAP

Realizado por: Adriana E. Yánez Tapia

Se realizó el escaneo de todos los servidores de Fundación ESPOIR con la Herramienta ZENMAP, como se puede observar en los Anexos 38 a 45, de los cuales se obtuvo la información mostrada en la Tabla 4.1.

Tabla 4.1 Resumen de información obtenida con la herramienta *ZE*NMAP

Resultados de la Herramienta ZENMAP en los Servidores de ESPOIR				
Servidor	**IP Local**	**Hostname**	**S.O.**	**Servicio**
Servidor de Base de Datos	192.168.0.15	qui-bdd	Microsoft Windows Server 2008 R2 Standard Service Pack 1	Microsoft SQL Server 2008 R2 SP1
Servidor de Aplicaciones	192.168.0.21		Linux 2.6.32	http-server (GlassFish Server Open Source Edition 5.0.1)
Servidor de Nómina	192.168.0.19	qui-n0mina	Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds	Servidor Web: Apache-Coyote/1.1
Servidor de Sistema Medico	192.168.0.18	qui-srvmed	Microsoft Windows Server 2008 R2 Standard Service Pack 1	Http Server (Apache Tomcat 2.4.10)
Servidor de Replicación	192.168.0.197	qui_veeam_srvr	Microsoft Windows Server 2008 R2 Standard Service Pack 1	
Servidor de Intranet	192.168.20.3	intranet	CentOS	Http (Joomla - Apache 2.2.15)
Servidor Web Services Produbanco	192.168.0.204		Microsoft Windows Server 2003 Service Pack 2	Microsoft IIS 6.0
Servidor Web Services Equifax	192.168.0.212	srv-wseqfx	Microsoft Windows Server 2012 R2 DataCenter	Microsoft IIS 8.5
Servidor página Web	192.168.0.2	www.espoir.org.ec	Centos	Http (Apache 2.2.15)

Realizado por: Adriana E. Yánez Tapia

Como resultados de las pruebas realizadas con la herramienta ZENMAP, se detectaron varios puertos abiertos como: 21 (FTP) , 22 (SSH), 25 (SMTP), 80 (HTTP para servidores Web), 110 (POP3), 135, 139, 445 (Asociados a Netbios), 1720 (Asociado a H323 tipo TCP), 3389 (Microsoft Remote Desktop), 8080 (HTTP para servidores Web Cache), en las reglas de navegación creadas en el PFSense se controló los puertos publicados, dejando abiertos solo los puertos necesarios. Los puertos abiertos para servicio Web, por medio de las reglas de PFSene son: 21 (FTP), 25 (SMTP), 80 (HTTP para servidores Web), 110 (POP3).

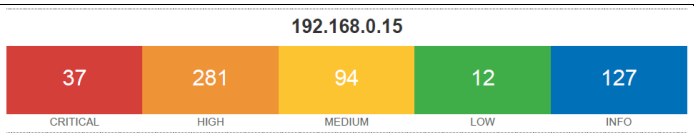
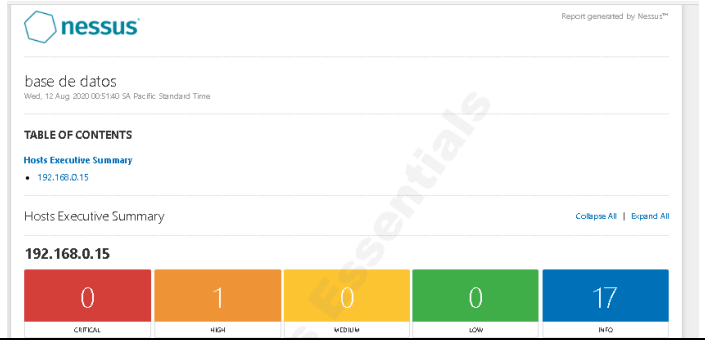
4.3.2 Análisis de vulnerabilidades posterior a la Implementación

Para la revisión de vulnerabilidades de los servidores de Fundación ESPOIR, se utilizaron las herramientas Nessus, NMAP, y NIKTO.

4.3.2.1 Análisis de Vulnerabilidades con NESSUS

Esta herramienta, nos permite apreciar los resultados en base a los colores, el nivel de criticidad de las vulnerabilidades detectadas en los servidores. En la Tabla 4.2, se muestra los resultados obtenidos con la herramienta Nessus, aplicada al Servidor de Base de Datos, se muestra el estado inicial antes de la solución PFSense y el análisis Final posterior a la implementación de la solución.

Tabla 4.2 Vulnerabilidades encontradas en el Servidor de Base de Datos con Nessus.

Servidor de Base de Datos	
Análisis de vulnerabilidades de escaneo interno	
Análisis Inicial	
Análisis Final	

Realizado por: Adriana E. Yánez Tapia

El Análisis de vulnerabilidades con la herramienta Nessus en todos los servidores de ESPOIR se los puede apreciar los Anexos 46 a 54.

4.3.2.2 Análisis de Vulnerabilidades con NMAP

Adicional a la revisión de vulnerabilidades con la herramienta NESSUS se realizó una revisión de vulnerabilidades con el comando "**nmap -sV --script vulners --scritp-args mincvss-5.0 servidor**", en la Figura 4.11 se puede observar el resultado del comando aplicado para el servidor de página web y de los demás servidores en los Anexos 55 a 62.

Figura 4.11 Vulnerabilidades en el Servidor de página Web con la herramienta NMAP

Realizado por: Adriana E. Yánez Tapia

4.3.2.3 Análisis de Vulnerabilidades con NIKTO

Con la herramienta de Nikto se realizó un análisis de las vulnerabilidades de los servidores que presentan un servicio relacionado a un servicio web. Nikto es una herramienta especializada en el escaneo de vulnerabilidades web, en la Figura 4.12, se observa el resultado del análisis en el servidor de página web y de los demás servidores en los Anexos 63 a 68.

Figura 4.12 Vulnerabilidades en el Servidor de página Web con la herramienta NIKTO

Realizado por: Adriana E. Yánez Tapia

Una vez concluido este análisis de vulnerabilidades, se ha realizado un cuadro resumen del número de vulnerabilidades encontradas por nivel de criticidad, en la Tabla 4.3, se muestra la comparativa entre las vulnerabilidades iniciales y la finales donde se puede ver la disminución en las vulnerabilidades.

Tabla 4.3 Número de Vulnerabilidades encontradas con Nessus en los Servidores

	NIVEL DE CRITICIDAD DE VULNERABILIDAD					
Servidor	**Escaneo**	**# Critical**	**#High**	**#Medium**	**#Low**	**#Info**
Servidor de Base de Datos	Inicial	37	281	94	12	127
	Final	0	1	0	0	17
Servidor de Aplicaciones	Inicial	0	0	1	2	24
	Final	0	0	0	0	16
Servidor Sistema de Nomina	Inicial	3	2	10	1	44
	Final	1	2	3	1	22
Servidor Sistema Medico	Inicial	12	18	36	1	50
	Final	6	15	17	0	18
Servidor de Replicación	Inicial	2	3	13	1	43
	Final	1	0	3	2	22
Servidor de Intranet	Inicial	0	0	2	2	29
	Final	0	0	0	3	19
Servidor Web Services Produbanco	Inicial	4	3	4	1	36
	Final	0	0	4	2	19
Servidor Web Services Equifax	Inicial	0	0	10	1	39
	Final	0	0	3	1	20
Servidor WEB (Escaneo Externo)	Inicial	0	0	3	3	27
	Final	0	0	2	0	13
Servidor WEB (Escaneo Interno)	Inicial	0	0	0	0	6
	Final	0	0	0	1	16

Realizado por: Adriana E. Yánez Tapia

4.4 Análisis de Riesgos posterior a la Implementación

Para el punto de análisis de riesgos posterior a la implementación, se reconoce, calcula y prioriza los riesgos de la red de Fundación ESPOIR, mediante la relación existente entre las amenazas y vulnerabilidades.

Esto tomando en cuenta la naturaleza de la organización, se califican a los agentes de amenaza y a las vulnerabilidades que podrían ser utilizadas por estos agentes, también las consecuencias, la probabilidad de ocurrencia de evento e impacto a la continuidad del negocio en caso de que el evento suceda.

4.4.1 Matriz de Riesgos Inherente y Residual

Para determinar el nivel de seguridad en la red, se empleó el método T-V (Threat Vulnerability), que fija un proceso de correlación entre las amenazas y vulnerabilidades con el Appliance que se encuentra en funcionamiento. En la Tabla 4.4, se presenta la Matriz de Riesgo Inherente y Residual, de acuerdo con el análisis de vulnerabilidades obtenidas por Nessus en el análisis posterior a la implementación de PFSense.

Tabla 4.4 Matriz de riesgos Inherentes y Residuales

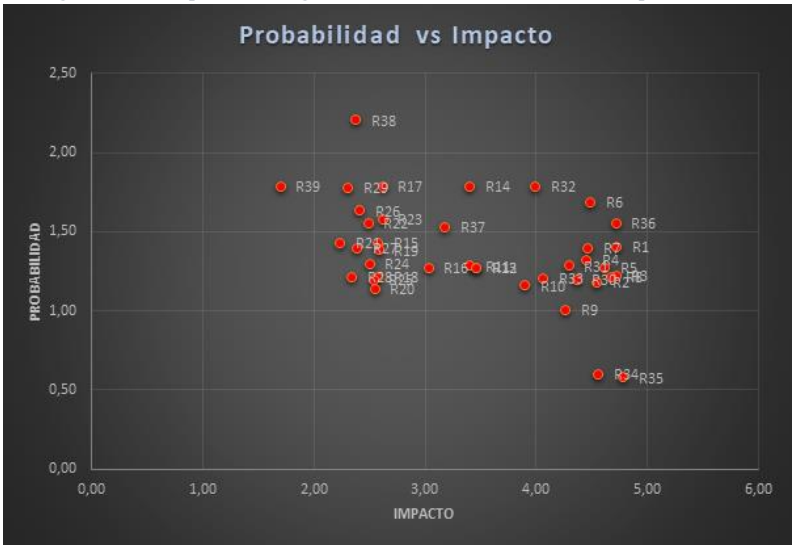
Servidor	Nivel de Criticidad	Descripción de Alerta	Etiqueta	Impacto	Probabilidad	Asociadas
Servidor de Base de Datos	Critica	Security Update	R1	4.73	1.40	15
	Critica	Could Allow Remote Code Execution	R2	4.55	1.17	13
	Critica	Unsupported Version Detection	R3	4.72	1.22	5
	Critica	uncredentialed check	R4	4.46	1.32	1
	Critica	Could Allow Elevation ofPrivilege	R5	4.62	1.27	3
	Alta	Security Update	R6	4.49	1.68	141
	Alta	Could Allow Remote Code Execution	R7	4.47	1.39	71
	Alta	Could Allow Elevation ofPrivilege	R8	4.68	1.21	53
	Alta	Could Allow Denial of Service	R9	4.27	1.00	16
Servidor de Nómina	Critica	Could Allow Remote Code Execution	R10	3.90	1.16	1
	Critica	uncredentialed check	R11	3.41	1.28	1
	Critica	Unsupported Version Detection	R12	3.47	1.27	1
	Alta	Could Allow Remote Code Execution	R13	3.47	1.27	1
	Alta	Security Update	R14	3.41	1.78	1
Servidor de Replicación	Critica	uncredentialed check	R15	2.58	1.43	1
	Critica	Unsupported Version Detection	R16	3.04	1.27	1
	Alta	Security Update	R17	2.63	1.78	1

	Alta	SSL Version 2 and 3 Protocol Detection	R18	2.58	1.21	1
	Alta	SMBv1 Vulnerabilities	R19	2.59	1.38	1
Servidor de Sistema Médico	Critica	Could Allow Remote Code Execution	R20	2.55	1.14	1
	Critica	uncredentialed check	R21	2.24	1.43	1
	Critica	OpenSSL 1.0.1	R22	2.50	1.55	3
	Critica	PHP 5.5.x Multiple Vulnerabilities	R23	2.63	1.58	6
	Critica	Unsupported Version Detection	R24	2.51	1.29	1
	Alta	Could Allow Remote Code Execution	R25	2.54	1.19	1
	Alta	Security Update	R26	2.42	1.63	1
	Alta	Apache 2.2.x Vulnerabilities	R27	2.39	1.39	2
	Alta	OpenSSL 1.0.1	R28	2.35	1.21	1
	Alta	PHP 5.5.x Multiple Vulnerabilities	R29	2.31	1.77	13
Servidor Web Services Produbanco	Critica	Unsupported Version Detection	R30	4.37	1.19	3
	Critica	uncredentialed check	R31	4.30	1.28	1
	Alta	Security Update	R32	4.00	1.78	1
	Alta	SMBv1 Vulnerabilities	R33	4.07	1.20	2
Catástrofes Naturales	Bajo		R34	4.56	0.59	1.00
Vandalismo/Robo	Bajo		R35	4.79	0.58	1.00
Cortes de Servicios de enlaces	Medio		R36	4.72	1.55	1.00
Cortes de energía eléctrica	Bajo		R37	3.19	1.53	1.00
WIFI	Medio		R38	2.38	2.20	1.00
Usuarios Externos	Medio		R39	1.71	1.78	1.00

Realizado por: Adriana E. Yánez Tapia

Para poder observar la distribución del Riesgo Total que es igual al producto del Impacto por la Probabilidad de ocurrencia se realizó un diagrama de Función Probabilidad vs Impacto.

Figura 4.13 Mapeo de Riesgos de Función Probabilidad vs Impacto Final



Realizado por: Adriana E. Yánez Tapia

4.4.2 Estrategia de Tratamiento de Riesgos

Como parte del proceso de tratamiento de los riesgos se aplicaron cuatro posibles acciones, las cuales tienen como objetivo el tratamiento del riesgo. Esas acciones son:

- Eliminar el riesgo
- Reducir el riesgo
- Transferir el riesgo
- Aceptar el riesgo

A continuación, se define las acciones tomadas en los riesgos existentes en Fundación ESPOIR.

Tabla 4.5 Matriz de riesgos Inherentes y Residuales con Estrategia de Tratamiento de Riesgos

Etiqueta	Servidor	Nivel Criticidad	Descripción de Alerta	Estrategia de Tratamiento
R1	Servidor de Base de Datos	Critica	Security Update	Eliminar
R2		Critica	Could Allow Remote Code Execution	Reducir
R3		Critica	Unsupported Version Detection	Aceptar
R4		Critica	uncredentialed check	Reducir
R5		Critica	Could Allow Elevation ofPrivilege	Reducir
R6		Alta	Security Update	Reducir
R7		Alta	Could Allow Remote Code Execution	Reducir
R8		Alta	Could Allow Elevation ofPrivilege	Reducir
R9		Alta	Could Allow Denial of Service	Reducir
R10	Servidor de Nómina	Critica	Could Allow Remote Code Execution	Reducir
R11		Critica	uncredentialed check	Reducir
R12		Critica	Unsupported Version Detection	Aceptar
R13		Alta	Could Allow Remote Code Execution	Reducir
R14		Alta	Security Update	Reducir
R15	Servidor de Replicación	Critica	uncredentialed check	Reducir
R16		Critica	Unsupported Version Detection	Aceptar
R17		Alta	Security Update SMB	Eliminar
R18		Alta	SSL Version 2 and 3 Protocol Detection	Eliminar
R19		Alta	SMBv1 Vulnerabilities	Eliminar
R20	Servidor de Sistema Médico	Critica	Could Allow Remote Code Execution	Reducir
R21		Critica	uncredentialed check	Reducir
R22		Critica	OpenSSL 1.0.1	Eliminar
R23		Critica	PHP 5.5.x Multiple Vulnerabilities	Reducir
R24		Critica	Unsupported Version Detection	Aceptar
R25		Alta	Could Allow Remote Code Execution	Reducir
R26		Alta	Security Update	Reducir
R27		Alta	Apache 2.2.x Vulnerabilities	Reducir
R28		Alta	OpenSSL 1.0.1	Eliminar
R29		Alta	PHP 5.5.x Multiple Vulnerabilities	Reducir
R30	Servidor Web Services Produbanco	Critica	Unsupported Version Detection	Aceptar
R31		Critica	uncredentialed check	Reducir
R32		Alta	Security Update	Eliminar
R33		Alta	SMBv1 Vulnerabilities	Eliminar
R34	Catastrofes Naturales	Bajo		Aceptar
R35	Vandalismo/Robo	Bajo		Aceptar
R36	Costes de Servicios de enlaces	Medio		Transferir
R37	Cortes de energia electrica	Bajo		Reducir
R38	WIFI	Medio		Transferir
R39	Usuarios Externos	Medio		Transferir

Realizado por: Adriana E. Yánez Tapia

4.4.3 Matriz de Riesgos Residual

Una vez que se aplican los controles sugeridos de seguridad, se puede verificar el cambio de la criticidad de los riesgos inherentes por cada una de las vulnerabilidades, además del cambio de la valoración del impacto y la probabilidad residuales, en la Tabla 4.6, se observa el detalle del riesgo residual.

Tabla 4.6 Matriz de riesgos Original y Residual

Original	Residual	Servidor/Servicio	Riesgo Inherente	Control Sugerido	Criticidad	Impacto Residual	Probabilidad Residual
R1		Servidor de Base de Datos	Critica	Actualizar	ninguna		
R2			Critica	Actualizar	ninguna		
R3	R1		Critica	Ninguno	Alta	4.72	1.22
R4			Critica	Actualizar	ninguna		
R5			Critica	Actualizar	ninguna		
R6			Alta	Actualizar	ninguna		
R7	R2		Alta	Actualizar	Medio	2.17	1.00
R8			Alta	Actualizar	ninguna		
R9			Alta	Actualizar	ninguna		
R10	R3	Servidor de Nomina	Critica	Actualizar	Critica	2.10	1.00
R11	R4		Critica	Actualizar	Alta	2.20	1.00
R12			Critica	Ninguno	ninguna		
R13	R5		Alta	Actualizar	Alta	2.00	1.00
R14			Alta	Actualizar	ninguna		
R15	R6	Servidor de Replicación	Critica	Actualizar	Critica	2.20	1.20
R16			Critica	Ninguno	ninguna		
R17			Alta	Desactivar SMB	ninguna		
R18			Alta	Desactivar Protocolo SSL	ninguna		
R19			Alta	Desactivar SMBv1	ninguna		
R20		Servidor de Sistema Médico	Critica	Actualizar	ninguna		
R21			Critica	Actualizar	ninguna		
R22			Critica	Desactivar Protocolo SSL	ninguna		
R23	R7		Critica	Actualizar	Critica	2.20	1.20
R24			Critica	Ninguno	ninguna		
R25			Alta	Actualizar	ninguna		
R26			Alta	Actualizar	ninguna		
R27	R8		Alta	Actualizar	Alta	2.00	1.00
R28			Alta	Desactivar Protocolo SSL	ninguna		
R29	R9		Alta	Actualizar	Medio	2.00	1.00
R30		Servidor Web Services Produbanco	Critica	Ninguno	ninguna		
R31			Critica	Actualizar	Medio	3.00	1.00
R32			Alta	Actualizar	Bajo	3.50	1.10
R33			Alta	Desactivar SMBv1	ninguna		
R34	R10	Catástrofes Naturales	Bajo	Ninguno	Bajo	4.56	0.59
R35	R11	Vandalismo/Robo	Bajo	Ninguno	Bajo	4.79	0.58
R36	R12	Costes de Servicios de enlaces	Medio	Redundancia de enlaces	Medio	3.50	1.55
R37	R13	Cortes de energía eléctrica	Bajo	UPS Central	Bajo	1.50	2.20

R38	R14	WIFI	Medio	Responsable de seguridad	Medio	2.30	2.00
R39	R15	Usuarios Externos	Medio	Responsable de seguridad	Medio	1.71	1.50

Realizado por: Adriana E. Yánez Tapia

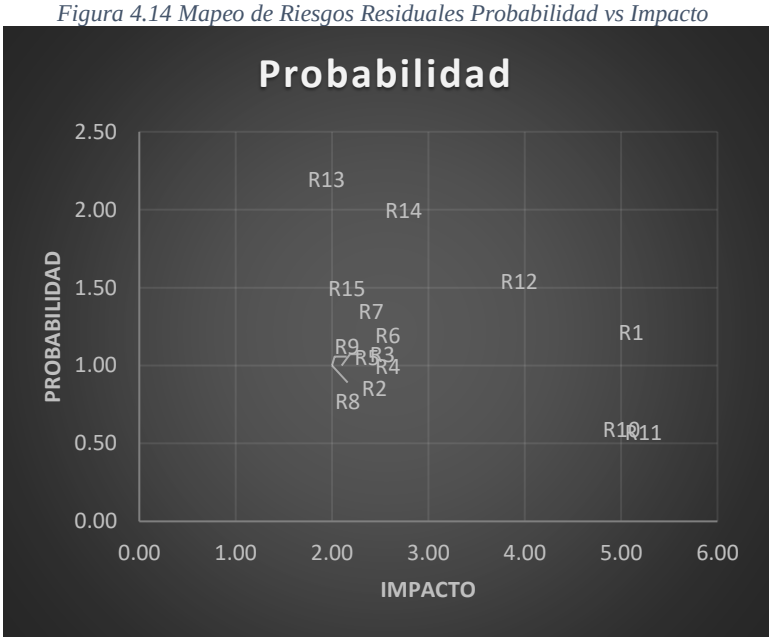
Tabla 4.7 Matriz de riesgos residual de vulnerabilidades

Residual	Riesgo Inherente	Riesgo Res	Impacto Res	Probabilidad Res
R1	Critica	Alta	4.72	1.22
R2	Alta	Medio	2.17	1.00
R3	Critica	Critica	2.10	1.00
R4	Critica	Alta	2.20	1.00
R5	Alta	Alta	2.00	1.00
R6	Critica	Critica	2.20	1.20
R7	Critica	Critica	2.20	1.20
R8	Alta	Alta	2.00	1.00
R9	Alta	Medio	2.00	1.00
R10	Bajo	Bajo	4.56	0.59
R11	Bajo	Bajo	4.79	0.58
R12	Medio	Medio	3.50	1.55
R13	Bajo	Bajo	1.50	2.20
R14	Medio	Medio	2.30	2.00
R15	Medio	Medio	1.71	1.50

Realizado por: Adriana E. Yánez Tapia

En la Figura 4.14, se presenta el diagrama de los riesgos residuales una vez aplicados los controles sugeridos, tomando en cuenta que el riesgo inicial fue categorizado para su tratamiento en una de estas estrategias: Eliminado, Reducido, Transferido o Aceptado.

Figura 4.14 Mapeo de Riesgos Residuales Probabilidad vs Impacto



Realizado por: Adriana E. Yánez Tapia

CONCLUSIONES

- Aun cuando ESPOIR cuenta con sistemas de seguridad para la gestión de antivirus y para monitorear su intranet corporativa; su operación y administración independiente provocaba que la gestión de la seguridad sea sesgada y dispersa, por lo cual la solución UTM permitió integrar y centralizar de forma eficiente el control de amenazas de la institución.

- El análisis de riesgos de seguridad realizado en la Fundación permitió caracterizar y evaluar sus activos tecnológicos y a partir de ello se priorizó los controles de seguridad necesarios para garantizar la operación normal y segura de su infraestructura informática.

- Para identificar las amenazas y vulnerabilidades en la red interna y externa de ESPOIR, se aplicaron test controlados de hacking ético, los cuales permitieron definir una línea base de operación para establecer un conjunto de políticas orientadas a salvaguardar la confidencialidad e integridad de la información.

- Gracias a que PFSense constituye un UTM basado en arquitectura open Source, su implementación en ESPOIR, representó una alternativa de gran relevancia por cuanto su coste de desarrollo es relativamente bajo y además ofrece iguales e incluso mejores funcionalidades y prestaciones que otras soluciones propietarias disponibles en el mercado.

RECOMENDACIONES

- Como complemento a la implementación del UTM, se recomienda la implementación de un firewall de capa 3, el cual permitirá administrar y filtrar los paquetes de una manera mucho más especializada, disminuyendo el riesgo de intrusiones externas.

- Se recomienda realizar, conjuntamente con el proveedor de la red WAN, una evaluación de los riesgos de seguridad en los enlaces de la matriz hacia las sucursales, a fin de garantizar la confidencialidad e integridad de la información corporativa.

- Considerando el incremento exponencial de las transacciones virtuales que se realizan actualmente en la fundación debido a la emergencia sanitaria, sería importante valorar el desempeño de los servidores, ya que sus características de hardware no brindan las garantías necesarias para procesar los altos volúmenes de información que hoy recibe la fundación.

BIBLIOGRAFÍA

Andalucia, e. D. (14 de junio de 2019). *Andalucia es Digital*. Obtenido de https://www.blog.andaluciaesdigital.es/pentesting-que-es/

Astudillo B., K. (2018). *Hacking Ético.* Madrid: RA-MA Editorial.

Esaú, A. (24 de 10 de 2018). *Open Webinars*. Obtenido de https://openwebinars.net/blog/que-es-el-pentesting/

ESPOIR, F. (2018). Obtenido de http://www.espoir.org.ec/misionvision.html

Incibe. (19 de 09 de 2019). *Instituto Nacional de Ciberseguridad*. Obtenido de https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

ISOToolsExcellence. (2018). *Blog Especializado en SGSI*. Obtenido de https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

Ostec. (04 de 01 de 2018). *Segurança digital de resultados*. Obtenido de https://ostec.blog/es/seguridad-perimetral/papel-del-firewall-utm

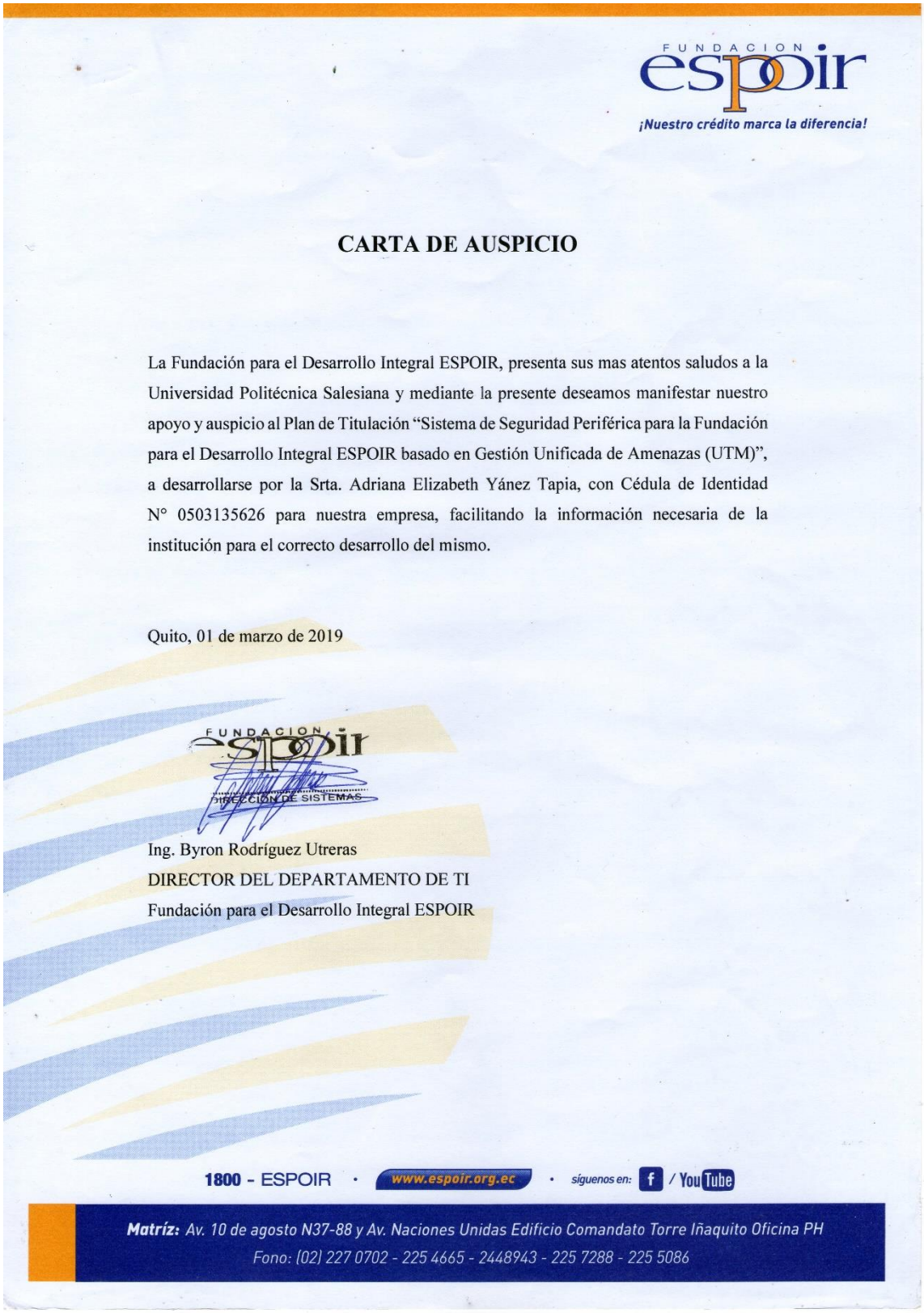
Poveda, I. J. (03 de 2011). *Analisis y valoracion de Riesgos*. Obtenido de https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf

Rio, F. d. (14 de julio de 2017). *Cero Uno Software Corporativo*. Obtenido de https://blog.cerounosoftware.com.mx/t%C3%A9rminos-de-seguridad-inform%C3%A1tica-glosario

System, O. (2016). *Glosario Seguridad ona System*. Obtenido de https://www.onasystems.net/wp-content/uploads/2016/10/Glosario-seguridad-Ona-systems-2016.pdf

Verdesoto, A. (octubre de 2007). *Biblioteca Digital EPN*. Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/548/1/CD-1053.pdf

ANEXO A



FUNDACION espoir

¡Nuestro crédito marca la diferencia!

CARTA DE AUSPICIO

La Fundación para el Desarrollo Integral ESPOIR, presenta sus mas atentos saludos a la Universidad Politécnica Salesiana y mediante la presente deseamos manifestar nuestro apoyo y auspicio al Plan de Titulación "Sistema de Seguridad Periférica para la Fundación para el Desarrollo Integral ESPOIR basado en Gestión Unificada de Amenazas (UTM)", a desarrollarse por la Srta. Adriana Elizabeth Yánez Tapia, con Cédula de Identidad N° 0503135626 para nuestra empresa, facilitando la información necesaria de la institución para el correcto desarrollo del mismo.

Quito, 01 de marzo de 2019

FUNDACION espoir
DIRECCIÓN DE SISTEMAS

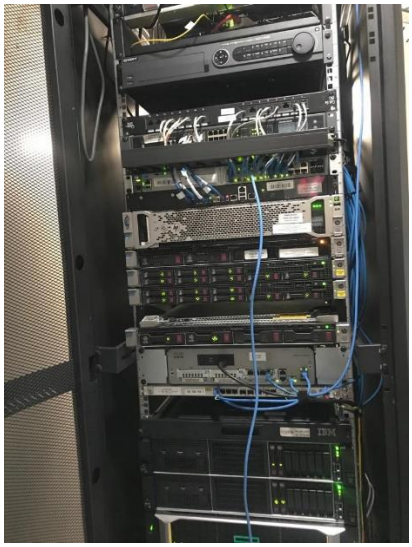
Ing. Byron Rodríguez Utreras
DIRECTOR DEL DEPARTAMENTO DE TI
Fundación para el Desarrollo Integral ESPOIR

1800 - ESPOIR · www.espoir.org.ec · síguenos en: / YouTube

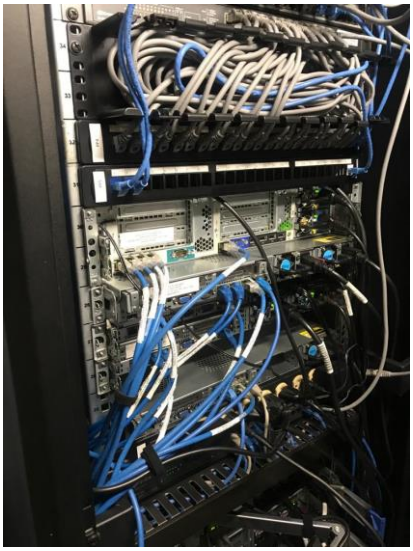
Matríz: Av. 10 de agosto N37-88 y Av. Naciones Unidas Edificio Comandato Torre Iñaquito Oficina PH
Fono: (02) 227 0702 - 225 4665 - 2448943 - 225 7288 - 225 5086

Anexo 1. Carta de Auspicio por parte de Fundación ESPOIR.

ANEXO B
LEVANTAMIENTO DE INFORMACION



Anexo 2. Fundación ESPOIR, Oficina Matriz, Data Center, Rack Servidores y Comunicación Referencial 1



Anexo 3. Fundación ESPOIR, Oficina Matriz, Data Center, Rack de Comunicaciones

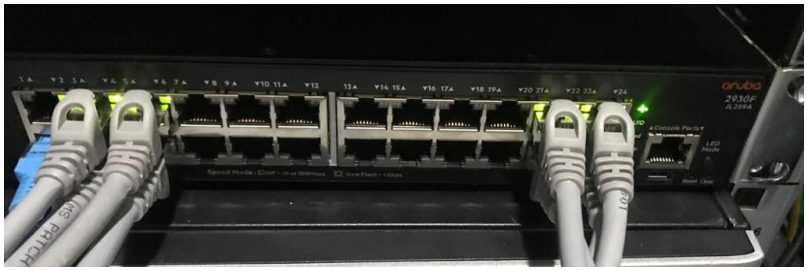
Anexo 4. Fundación ESPOIR, Oficina Matriz, Data Center, Sistema de Climatización

Anexo 5. Fundación ESPOIR, Oficina Matriz, Data Center Equipo de Comunicaciones, Central Telefónica IP GrandStream UCM-6116

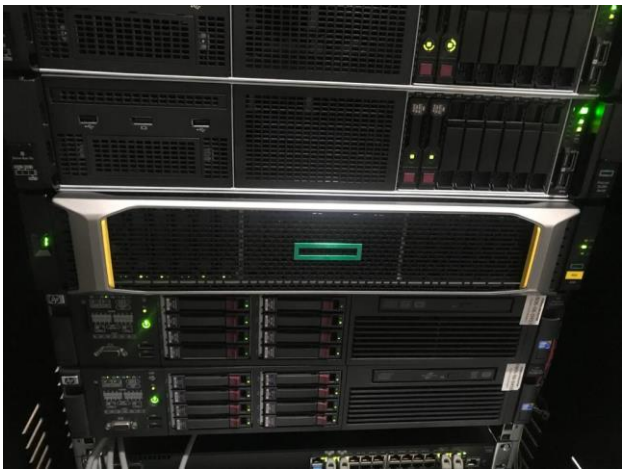
Anexo 6. Fundación ESPOIR, Oficina Matriz, Data Center, Equipo de Vieo Vigilancia, DVR EPCOM 24-Channel

Anexo 7. Fundación ESPOIR, Oficina Matriz, Data Center, Equipo de Comunicación, Router Cisco 1800 Series

Anexo 8. Fundación ESPOIR, Oficina Matriz, Data Center, Equipo de Comunicación, Switch HP 2920-24G J9726A



Anexo 9. Fundación ESPOIR, Oficina Matriz, Data Center, Equipo de Comunicación, Switch ARUBA 2930-F JL-259A



Anexo 10. Fundación ESPOIR, Oficina Matriz, Data Center, Equipos Servidores HP

Anexo 11. Fundación ESPOIR, Oficina Matriz, 4to Piso, Equipos de Comunicación, Rack 1

Anexo 12. Fundación ESPOIR, Oficina Matriz, 4to Piso, Equipos de Comunicación, Rack 2

ANEXO C

PRUEBAS DE PENTESTING

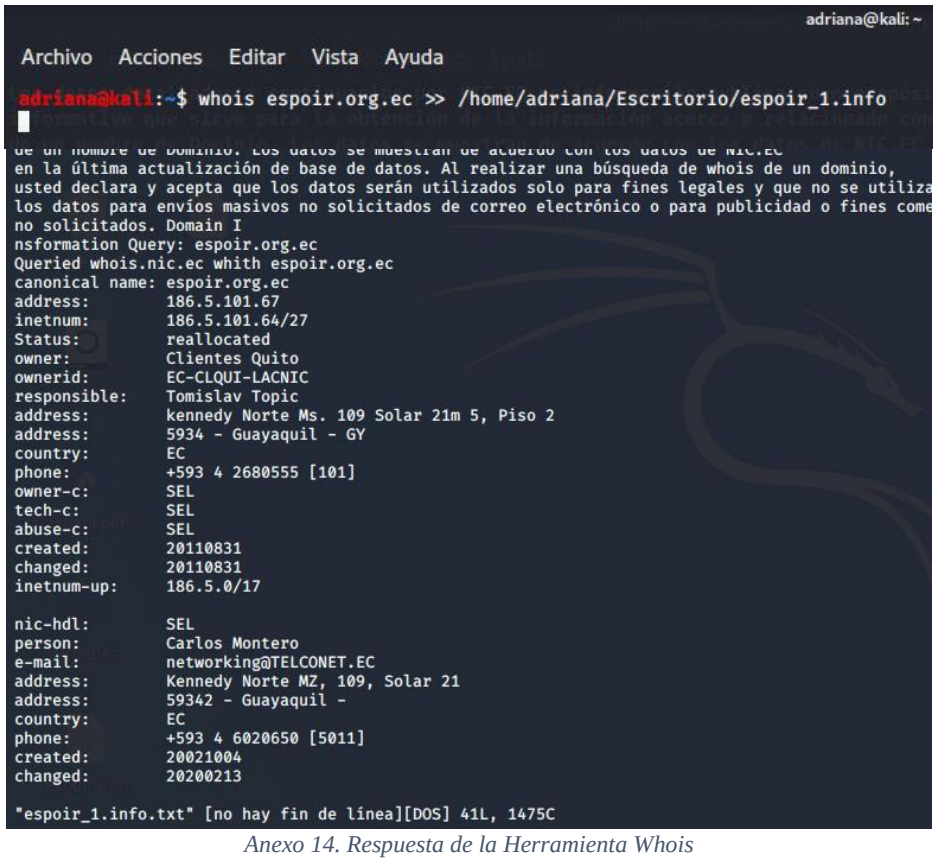
Geolocation data from ipinfo.io (Product: API, real-time)

IP Address	Country	Region	City
186.5.101.67	Ecuador	Pichincha	Quito
ISP	**Organization**	**Latitude**	**Longitude**
Telconet S.A	Telconet S.A (telconet.ec)	-0.2298	-78.5250

Geolocation data from DB-IP (Product: Full, 2020-8-1)

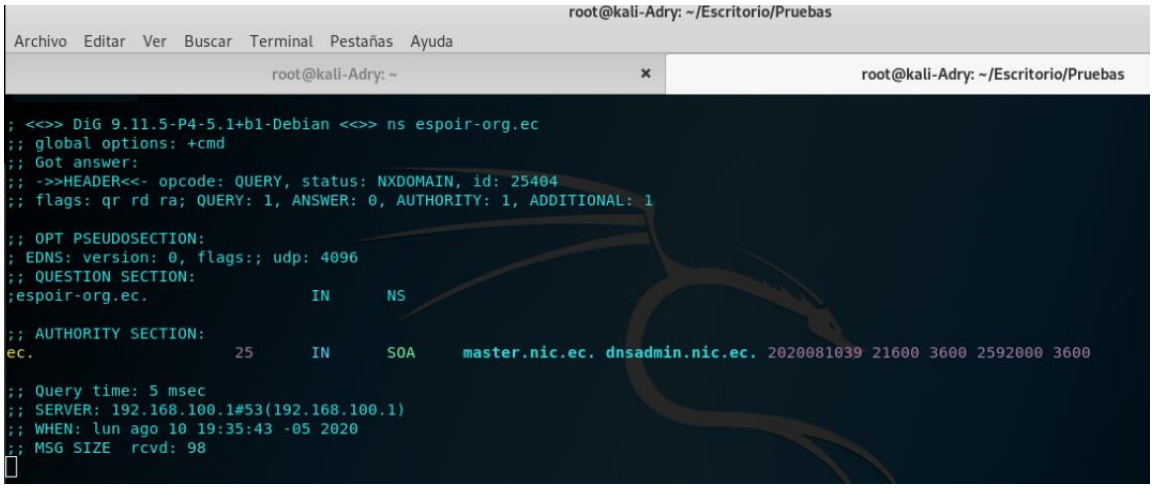
IP Address	Country	Region	City
186.5.101.67	Ecuador	Pichincha	Quito
ISP	**Organization**	**Latitude**	**Longitude**
Telconet S.A	Clientes Quito	-0.180653	-78.4678

Anexo 13. Geolocalización con www.iplocation.net de la IP 186.5.101.67



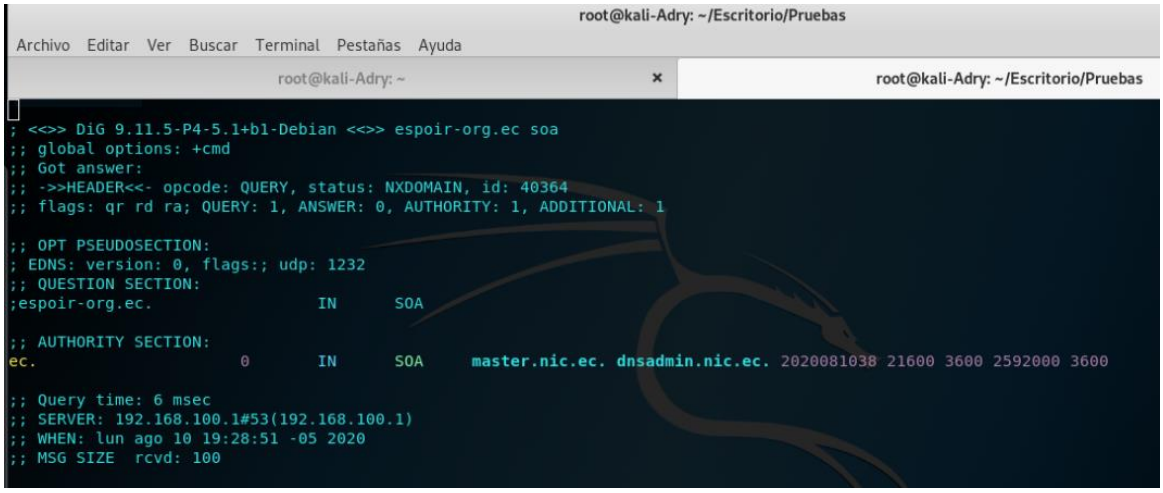
Anexo 14. Respuesta de la Herramienta Whois

Anexo 15. Herramientas Kali Linux, DIG, comando "dig ns espoir.org.ec >> /destino/nombre_archivo.info"



Anexo 16. Herramientas Kali Linux, DIG, respuesta a comando "dig ns espoir.org.ec >> /destino/nombre_archivo.info"

Anexo 17. Herramientas Kali Linux, DIG, comando "dig espoir.org.ec soa >> /destino/nombre_archivo.info"



Anexo 18. Herramientas Kali Linux, DIG, respuesta a comando "dig espoir.org.ec soa >> /destino/nombre_archivo.info"

192.168.0.15 / qui-bdd.espoir.local

Address

- 192.168.0.15 (ipv4)

Hostnames

- qui-bdd.espoir.local (PTR)

Ports

The 989 ports scanned but not shown below are in state: **closed**

- 989 ports replied with: **resets**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product
25	tcp	open	smtp	syn-ack	
	fingerprint-strings	NULL: 421 No SMTP service here			
	smtp-commands	SMTP EHLO qui-bdd.espoir.local: failed to receive data: failed to receive data			
80	tcp	open	http	syn-ack	Microsoft IIS httpd
	http-methods	Supported Methods: OPTIONS TRACE GET HEAD POST Potentially risky methods: TRACE			
	http-server-header	Microsoft-IIS/7.5			

Anexo 19. Información Obtenida del Servidor de Base de Datos con la Herramienta NMAP

192.168.0.21

Address

- 192.168.0.21 (ipv4)

Ports

The 993 ports scanned but not shown below are in state: **closed**

- 993 ports replied with: **resets**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	OpenSSH	5.3	protocol 2.0
	ssh-hostkey	1024 e2:52:87:49:c6:56:98:bc:5b:f0:2f:02:8e:3e:b7:15 (DSA) 2048 e9:4e:11:0e:e6:fd:81:ac:72:ba:9d:e5:f3:8d:4c:42 (RSA)					
25	tcp	open	smtp	syn-ack			
	fingerprint-strings	LDAPBindReq, NULL, SMBProgNeg, TerminalServerCookie: 421 No SMTP service here					
	smtp-commands	SMTP EHLO nmap.scanme.org: failed to receive data: failed to receive data					
80	tcp	open	http	syn-ack	Oracle GlassFish	5.0.1	Servlet 3.1; JSP 2.3; Java 1.8
	http-methods	Supported Methods: GET HEAD POST PUT DELETE TRACE OPTIONS Potentially risky methods: PUT DELETE TRACE					

Anexo 20.Información obtenida del Servidor de Aplicaciones con la herramienta NMAP

192.168.0.19 / qui-n0mina.espoir.local

Address

- 192.168.0.19 (ipv4)

Hostnames

- qui-n0mina.espoir.local (PTR)

Ports

The 992 ports scanned but not shown below are in state: **filtered**

- 992 ports replied with: **no-responses**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product
25	tcp	open	smtp	syn-ack	
	smtp-commands	SMTP EHLO qui-n0mina.espoir.local: failed to receive data: failed to receive data			
110	tcp	open	pop3	syn-ack	
135	tcp	open	msrpc	syn-ack	
445	tcp	open	microsoft-ds	syn-ack	Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds
1720	tcp	open	h323q931	syn-ack	
3389	tcp	open	ms-wbt-server	syn-ack	

Anexo 21. Información obtenida del Servidor de Nómina con la herramienta NMAP

192.168.0.18 / qui-srvmed.espoir.local

Address

- 192.168.0.18 (ipv4)

Hostnames

- qui-srvmed.espoir.local (PTR)

Ports

The 988 ports scanned but not shown below are in state: **filtered**

- 988 ports replied with: **no-responses**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product
25	tcp	open	smtp	syn-ack	
	smtp-commands	SMTP EHLO qui-srvmed.espoir.local: failed to receive data: failed to receive data			
80	tcp	open	http	syn-ack	Apache httpd
	http-favicon	Unknown favicon MD5: 3BD2EC61324AD4D27CB7B0F484CD4289			
	http-methods	Supported Methods: GET HEAD POST OPTIONS			
	http-server-header	Apache/2.4.10 (Win32) OpenSSL/1.0.1i PHP/5.5.15			
	http-title	Access forbidden! Requested resource was http://qui-srvmed.espoir.local/xampp/			

Anexo 22. Información obtenida del Servidor del Sistema Médico con la herramienta NMAP

192.168.0.197 / qui_veeam_srvr.espoir.local

Address

- 192.168.0.197 (ipv4)

Hostnames

- qui_veeam_srvr.espoir.local (PTR)

Ports

The 984 ports scanned but not shown below are in state: **closed**

- 984 ports replied with: **resets**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product
25	tcp	open	smtp	syn-ack	
	fingerprint-strings	FourOhFourRequest, LDAPSearchReq, NULL: 421 No SMTP service here			
	smtp-commands	SMTP EHLO qui_veeam_srvr.espoir.local: failed to receive data: failed to receive data			
110	tcp	open	pop3	syn-ack	
	fingerprint-strings	DNSStatusRequestTCP, FourOhFourRequest, Help, LANDesk-RC, LDAPBindReq, NULL, RPCCheck, SIPOptions, TerminalServerCookie, WMSReques -ERR No POP3 service here			
111	tcp	open	rpcbind	syn-ack	
135	tcp	open	msrpc	syn-ack	
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn
445	tcp	open	microsoft-ds	syn-ack	Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds
1063	tcp	open	rpcbind	syn-ack	

Anexo 23. Información obtenida del Servidor de Replicación con la herramienta NMAP

192.168.20.3 / intranet.espoir.local

Address

- 192.168.20.3 (ipv4)
- 00:50:56:98:0E:75 - VMware (mac)

Hostnames

- intranet.espoir.local (PTR)

Port		State (toggle closed [0] | filtered [0])	Service
22	tcp	open	ssh
80	tcp	open	http
	http-favicon	Unknown favicon MD5: 7557A6DE85C74BF99DDDFB5871CE30DE	
	http-generator	Joomla! - Open Source Content Management	
	http-methods	Supported Methods: GET HEAD POST OPTIONS	
	http-robots.txt	16 disallowed entries (15 shown) /joomla/administrator/ /administrator/ /cache/ /cli/ /components/ /images/ /includes/ /installation/ /language/ /libraries/ /logs/ /media/ /modules/ /plugins/ /templates/	
	http-server-header	Apache/2.2.15 (CentOS)	
	http-title	IntraNet ESPOIR	

Anexo 24. Información obtenida del Servidor de Sistema de Intranet con la herramienta NMAP

192.168.0.204

Address

- 192.168.0.204 (ipv4)

Ports

The 991 ports scanned but not shown below are in state: **closed**

- 991 ports replied with: **resets**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product
25	tcp	open	smtp	syn-ack	
	fingerprint-strings	Hello, NULL: 421 No SMTP service here			
	smtp-commands	SMTP EHLO nmap.scanme.org: failed to receive data: failed to receive data			
80	tcp	open	http	syn-ack	Microsoft IIS httpd
	http-methods	Supported Methods: OPTIONS TRACE GET HEAD POST Potentially risky methods: TRACE			
	http-server-header	Microsoft-IIS/6.0			

Anexo 25. Información obtenida del Servidor Web Services Produbanco con la herramienta NMAP

192.168.0.212 / srv-wseqfx.espoir.local

Address

- 192.168.0.212 (ipv4)

Hostnames

- srv-wseqfx.espoir.local (PTR)

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product
25	tcp	open	smtp	syn-ack	
80	tcp	open	http	syn-ack	Microsoft IIS httpd
	http-methods	Supported Methods: OPTIONS TRACE GET HEAD POST Potentially risky methods: TRACE			
	http-server-header	Microsoft-IIS/8.5			
	http-title	IIS Windows Server			
110	tcp	open	pop3	syn-ack	
135	tcp	open	msrpc	syn-ack	
445	tcp	open	microsoft-ds	syn-ack	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1027	tcp	open	msrpc	syn-ack	Microsoft Windows RPC
1030	tcp	open	msrpc	syn-ack	Microsoft Windows RPC
1720	tcp	open	h323q931	syn-ack	
1801	tcp	open	msmq	syn-ack	
2103	tcp	open	msrpc	syn-ack	Microsoft Windows RPC
2105	tcp	open	msrpc	syn-ack	Microsoft Windows RPC
2107	tcp	open	msrpc	syn-ack	Microsoft Windows RPC
3389	tcp	open	ms-wbt-server	syn-ack	

Anexo 26. Información obtenida del Servidor Web Services Equifax con la herramienta NMAP

192.168.0.2 / www.espoir.org.ec

Address

- 192.168.0.2 (ipv4)

Hostnames

- www.espoir.org.ec (PTR)

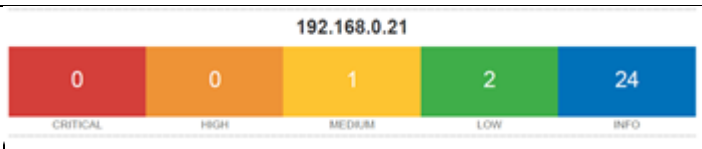
Port		State (toggle closed [10] | filtered [0])
21	tcp	open
22	tcp	open
25	tcp	open
80	tcp	open
	http-favicon	Unknown favicon MD5: D149D2B276F751BD080B7BCE4178AA9D
	http-generator	2018.1.1.386
	http-methods	Supported Methods: GET HEAD POST OPTIONS TRACE Potentially risky methods: TRACE
	http-server-header	Apache/2.2.15 (CentOS)

Anexo 27. Información obtenida del Servidor Web con la herramienta NMAP

Servidor de Aplicaciones

Host Details

IP:	192.168.0.21
OS:	Linux Kernel 2.6
Start:	March 18 at 12:06 AM
End:	March 18 at 12:12 AM
Elapsed:	6 minutes



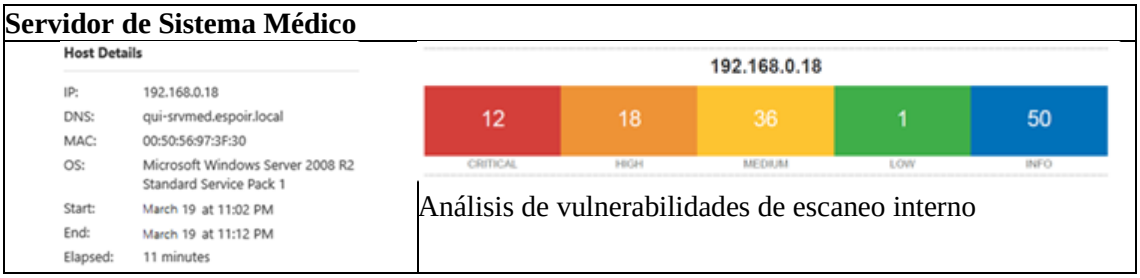
Análisis de vulnerabilidades de escaneo interno

Anexo 28. Herramienta NESSUS, Vulnerabilidades encontradas en el Servidor de Aplicaciones.

Servidor de Nómina

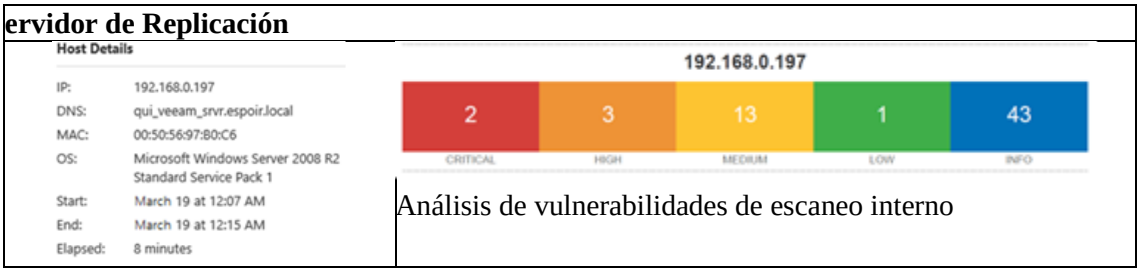
Anexo 29.Herramienta NESSUS, Vulnerabilidades encontradas en el Servidor de Nómina.

Servidor de Sistema Médico



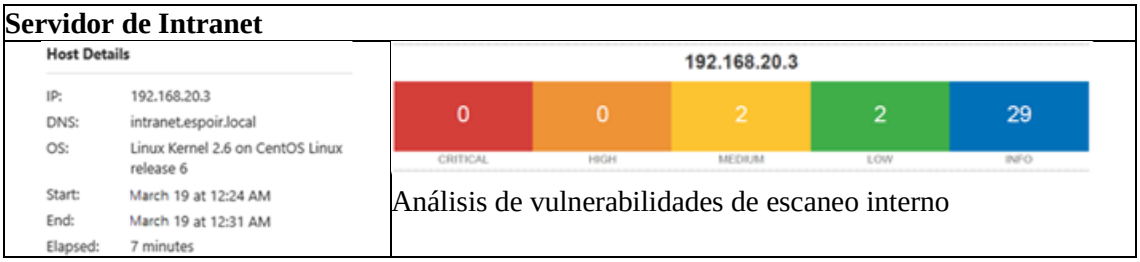
Anexo 30. Herramienta NESSUS, Vulnerabilidades encontradas en el Servidor de Sistema.

ervidor de Replicación



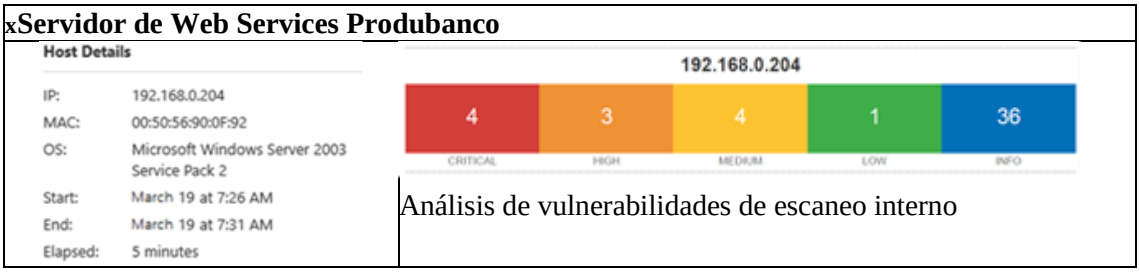
Anexo 31. Herramienta NESSUS, Vulnerabilidades encontradas en el Servidor de Replicación.

Servidor de Intranet



Anexo 32. Herramienta NESSUS, Vulnerabilidades encontradas en el Servidor de Intranet.

xServidor de Web Services Produbanco



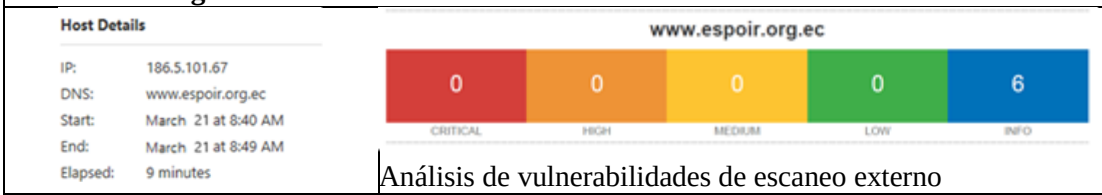
Anexo 33. Herramienta NESSUS, Vulnerabilidades encontradas en el Servidor Web Services de Produbanco.

Servidor de Web Services Equifax

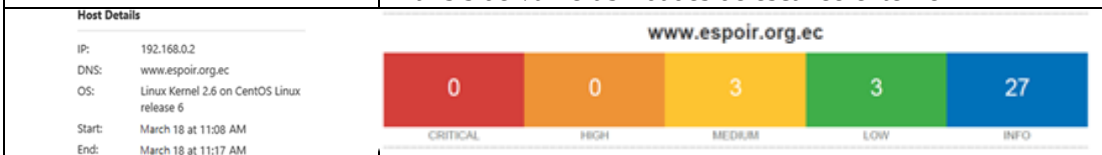
Análisis de vulnerabilidades de escaneo interno

Anexo 34. Herramienta NESSUS, Vulnerabilidades encontradas en el Servidor Web Services Equifax.

Servidor de Pagina Web

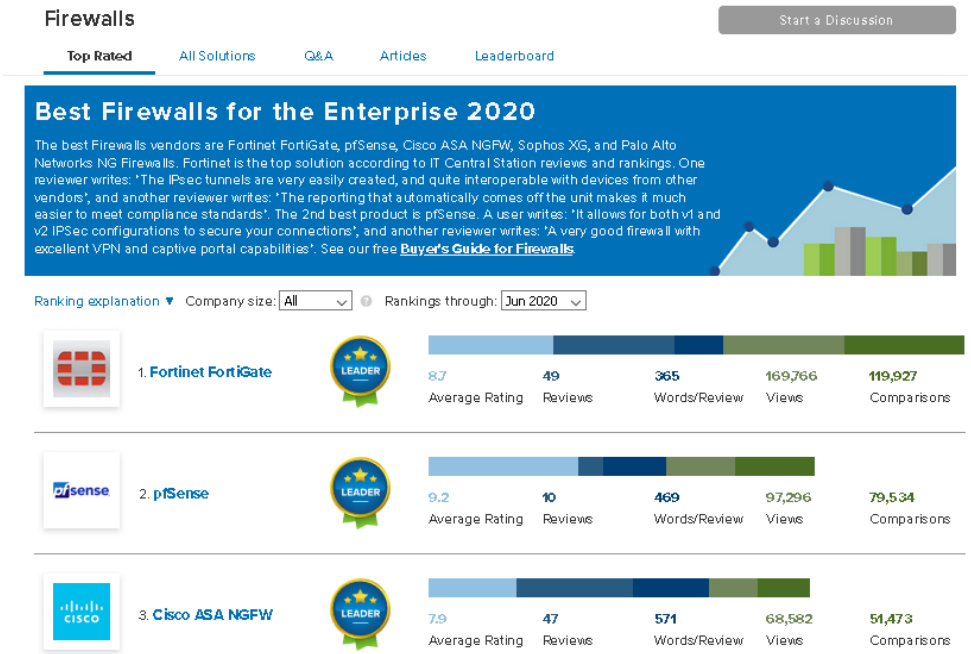


Análisis de vulnerabilidades de escaneo externo



Análisis de vulnerabilidades de escaneo interno

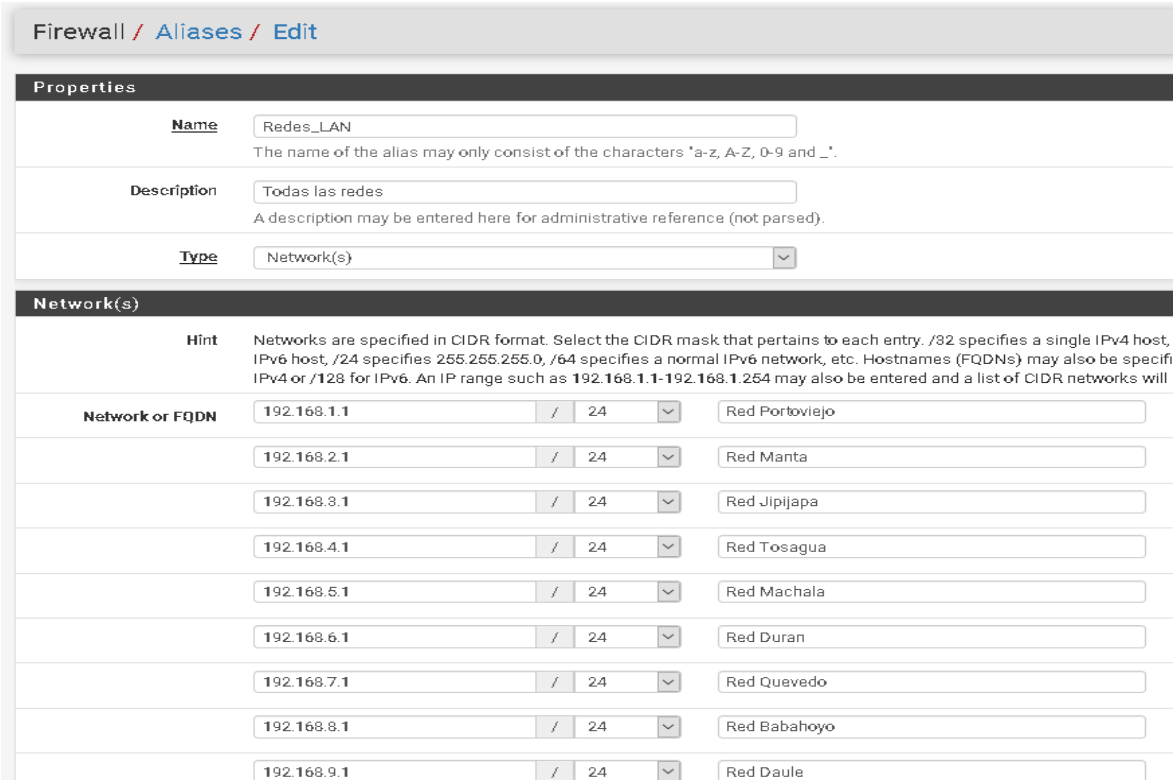
Anexo 35. Vulnerabilidades encontradas en el Servidor de la página Web con la herramienta Nessus.



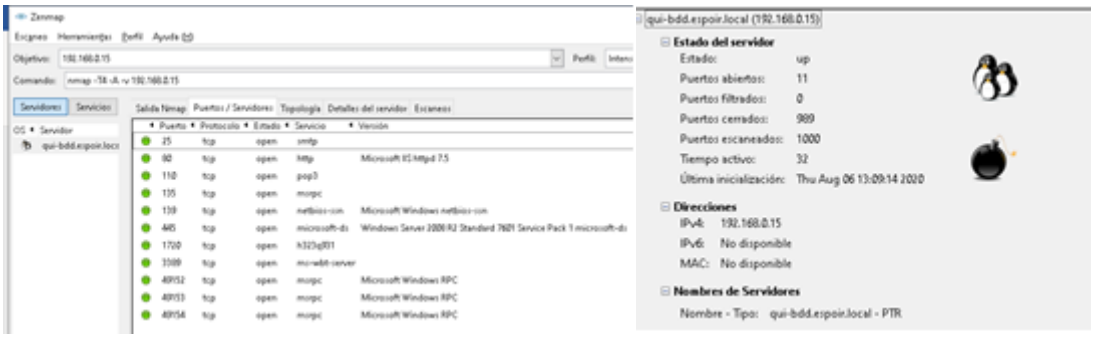
Anexo 36. Ranking de Firewalls en el Mercado Fuente IT Central Station.

ANEXO D

IMPLEMENTACIÓN DE LA SOLUCIÓN UTM

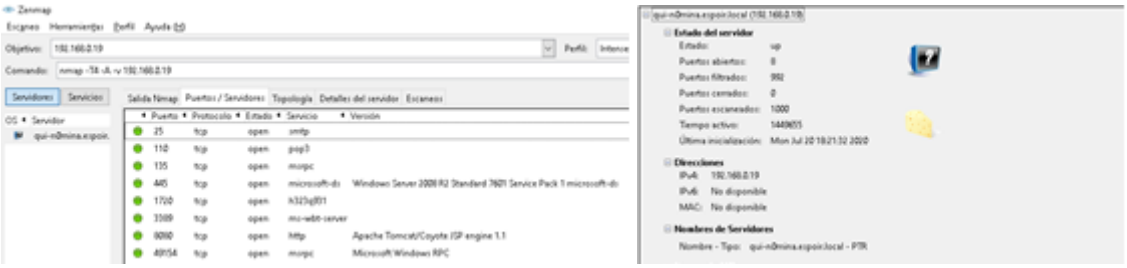


Anexo 37. Definición de ALIAS para redes LAN de sucursales

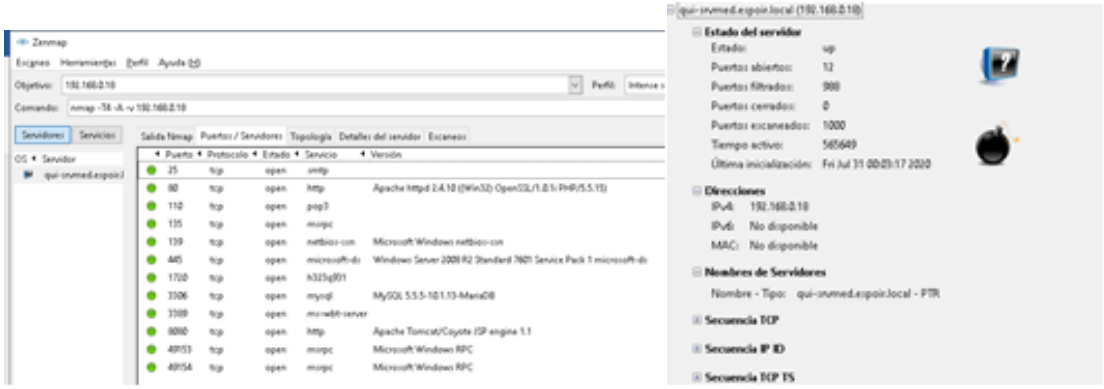


Anexo 38. Información obtenida del Servidor de Base de Datos con la herramienta ZENMAP

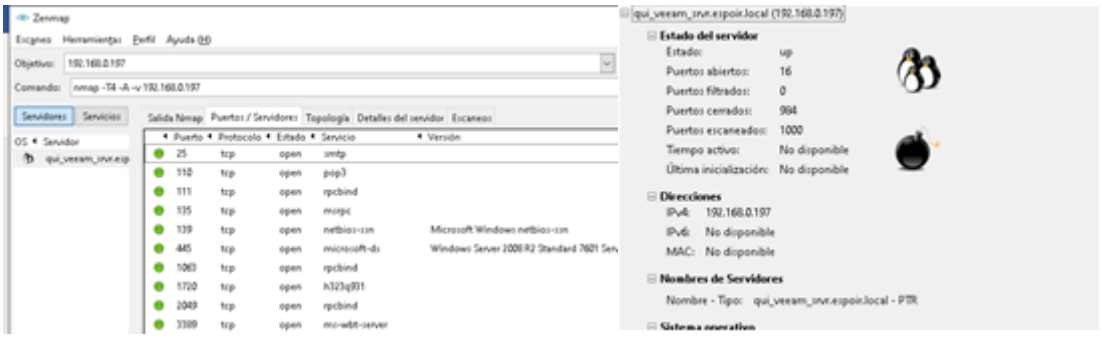
Anexo 39. Información obtenida del Servidor de Aplicaciones con la herramienta ZENMAP



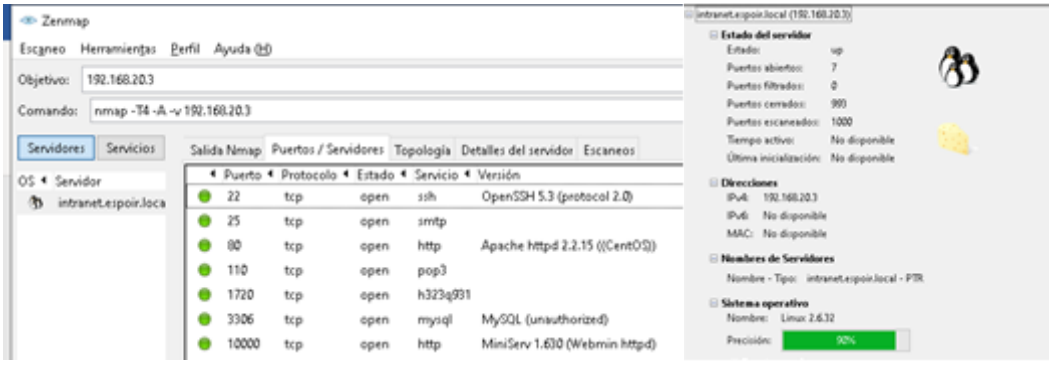
Anexo 40. Información obtenida del Servidor de Nomina con la herramienta ZENMAP



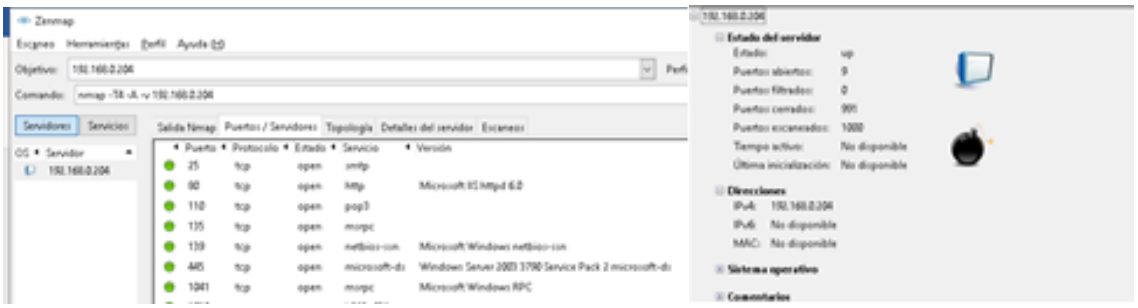
Anexo 41. Información obtenida del Servidor del Sistema Medico con la herramienta ZENMAP



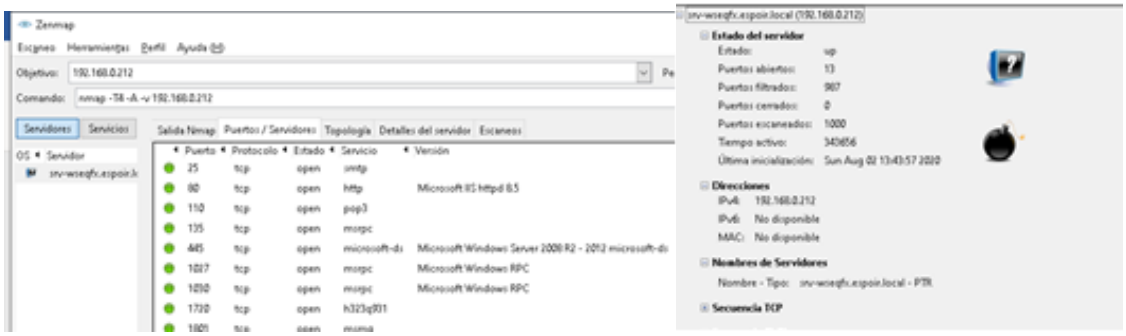
Anexo 42. Información obtenida del Servidor de Sistema de Replicación con la herramienta ZENMAP



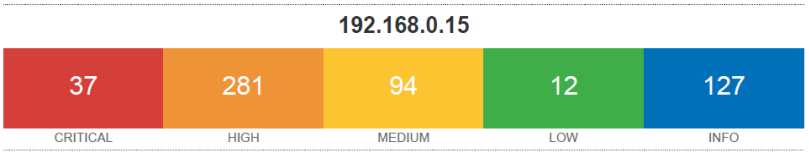
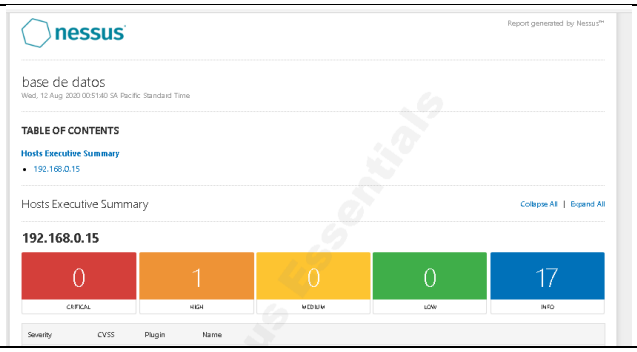
Anexo 43. Información obtenida del Servidor de Sistema de Intranet con la herramienta ZENMAP



Anexo 44. Información obtenida del Servidor Web Services Produbanco con la herramienta ZENMAP



Anexo 45. Información obtenida del Servidor Web Services Equifax con la herramienta ZENMAP

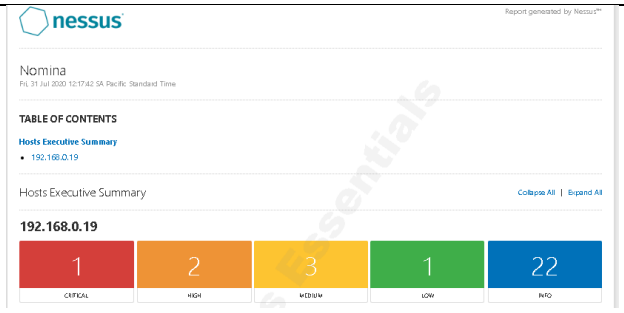
Servidor de Base de Datos	
Análisis de vulnerabilidades de escaneo interno	
Análisis Inicial	
Análisis Final	

Anexo 46. Vulnerabilidades encontradas en el Servidor de Base de Datos con la herramienta Nessus.

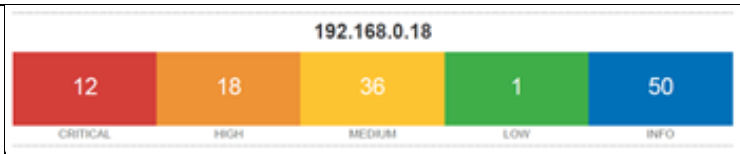
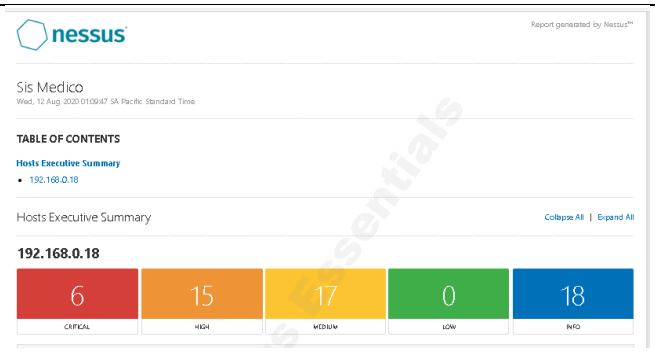
Servidor de Aplicaciones	
Análisis de vulnerabilidades de escaneo interno	
Análisis Inicial	

Análisis Final	

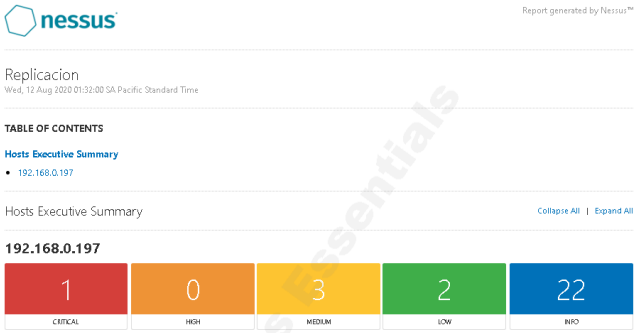
Anexo 47. Vulnerabilidades encontradas en el Servidor de Aplicaciones con la herramienta Nessus.

Servidor de Nómina	
Análisis de vulnerabilidades de escaneo interno	
Análisis Inicial	
Análisis Final	

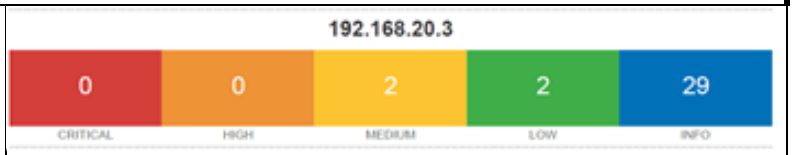
Anexo 48. Vulnerabilidades encontradas en el Servidor de Nómina con la herramienta Nessus.

Servidor de Sistema Médico	
Análisis de vulnerabilidades de escaneo interno	
Análisis Inicial	
Análisis Final	

Anexo 49. Vulnerabilidades encontradas en el Servidor de Sistema Médico con la herramienta Nessus.

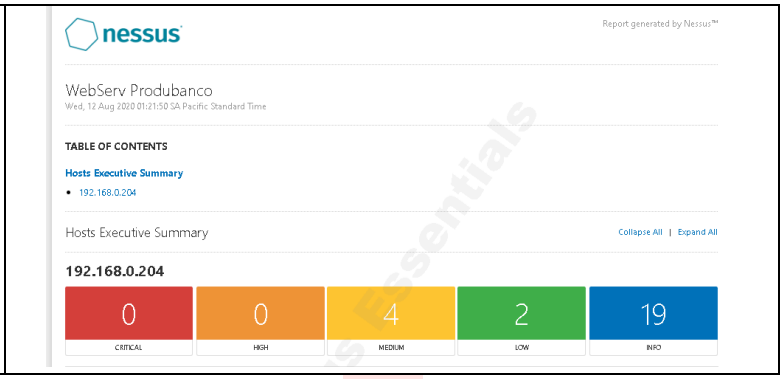
Servidor de Replicación	
Análisis de vulnerabilidades de escaneo interno	
Análisis Inicial	
Análisis Final	

Anexo 50. Vulnerabilidades encontradas en el Servidor de Replicación con la herramienta Nessus.

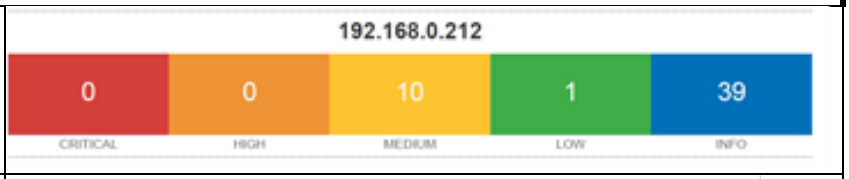
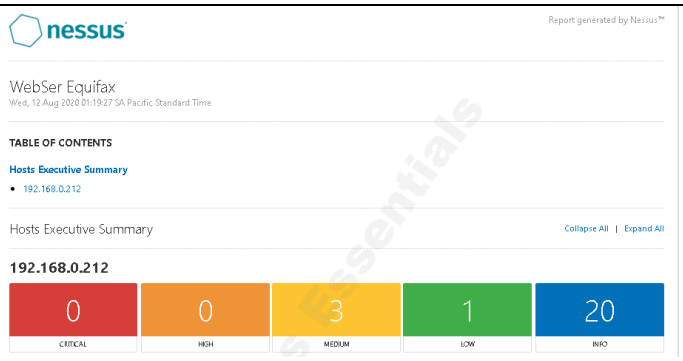
Servidor de Intranet	
Análisis de vulnerabilidades de escaneo interno	
Análisis Inicial	
Análisis Final	

Anexo 51. Vulnerabilidades encontradas en el Servidor de Intranet con la herramienta Nessus.

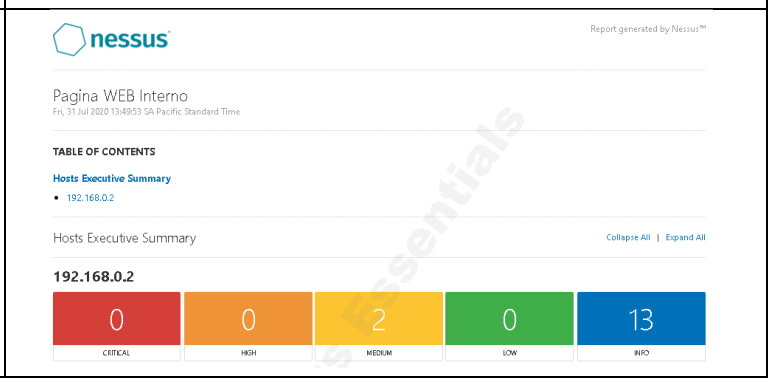
Servidor de Web Services Produbanco	
Análisis de vulnerabilidades de escaneo interno	
Análisis Inicial	

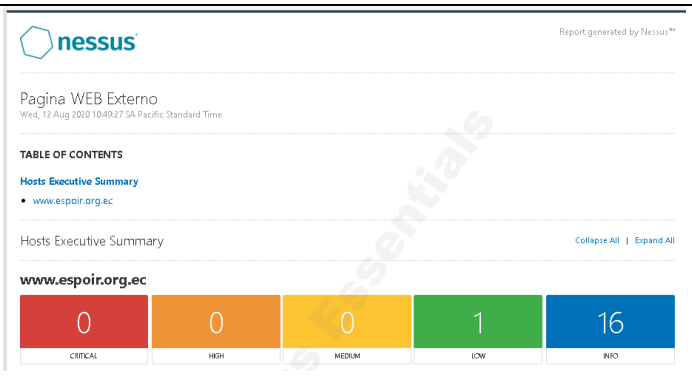
Análisis Final	

Anexo 52. Vulnerabilidades encontradas en el Servidor Web Services de Produbanco con la herramienta Nessus.

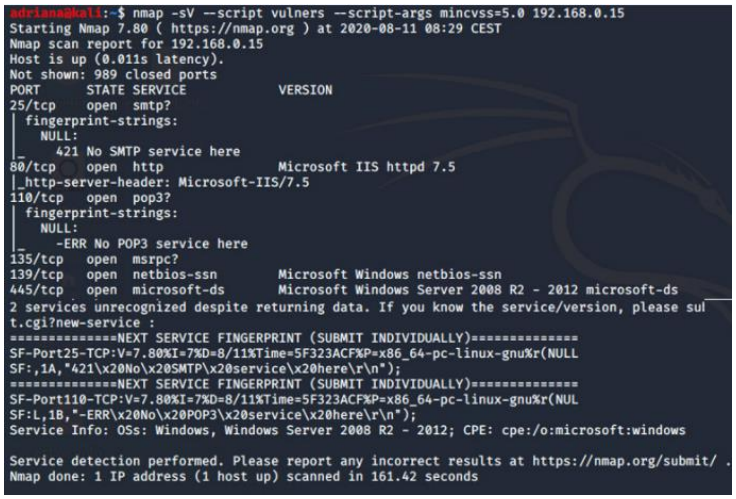
Servidor de Web Services Equifax	
Análisis de vulnerabilidades de escaneo interno	
Análisis Inicial	
Análisis Final	

Anexo 53. Vulnerabilidades encontradas en el Servidor Web Services Equifax con la herramienta Nessus.

Servidor de Web	
Análisis de vulnerabilidades de escaneo interno y externo	
Análisis Inicial interno	
Análisis Final interno	

Análisis Inicial externo	
Análisis Final externo	

Anexo 54. Vulnerabilidades encontradas en el Servidor de la página Web con la herramienta Nessus.



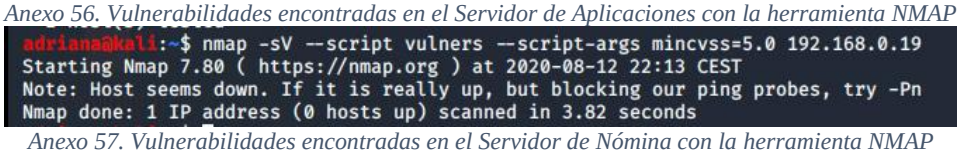
```
adriana@kali:~$ nmap -sV --script vulners --script-args mincvss=5.0 192.168.0.15
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-11 08:29 CEST
Nmap scan report for 192.168.0.15
Host is up (0.011s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE           VERSION
25/tcp    open  smtp?
| fingerprint-strings:
|   NULL:
|_    421 No SMTP service here
80/tcp    open  http              Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
110/tcp   open  pop3?
| fingerprint-strings:
|   NULL:
|_    -ERR No POP3 service here
135/tcp   open  msrpc?
139/tcp   open  netbios-ssn       Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds      Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
2 services unrecognized despite returning data. If you know the service/version, please sul
t.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port25-TCP:V=7.80%I=7%D=8/11%Time=5F323ACF%P=x86_64-pc-linux-gnu%r(NULL
SF:,1A,"421\x20No\x20SMTP\x20service\x20here\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port110-TCP:V=7.80%I=7%D=8/11%Time=5F323ACF%P=x86_64-pc-linux-gnu%r(NUL
SF:L,1B,"-ERR\x20No\x20POP3\x20service\x20here\r\n");
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 161.42 seconds
```

Anexo 55. Vulnerabilidades encontradas en el Servidor de Base de datos con la herramienta NMAP

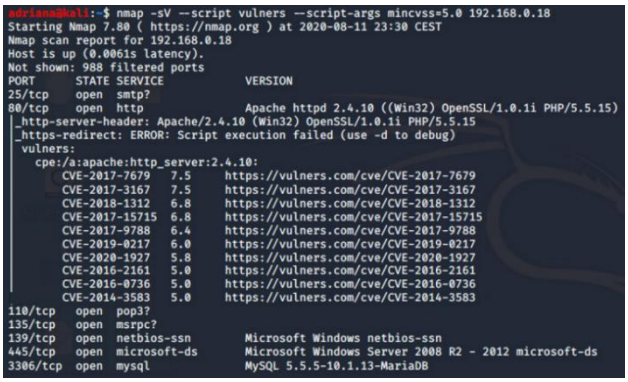
```
[redacted]:~$ nmap -sV --script vulners --script-args mincvss=5.0 192.168.0.21
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-11 08:35 CEST
Nmap scan report for 192.168.0.21
Host is up (0.011s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 5.3 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:5.3:
|       CVE-2010-4478   7.5     https://vulners.com/cve/CVE-2010-4478
|       CVE-2020-15778  6.8     https://vulners.com/cve/CVE-2020-15778
|       CVE-2017-15906  5.0     https://vulners.com/cve/CVE-2017-15906
|       CVE-2016-10708  5.0     https://vulners.com/cve/CVE-2016-10708
|_      CVE-2010-5107   5.0     https://vulners.com/cve/CVE-2010-5107
25/tcp   open  smtp?
| fingerprint-strings:
|   NULL:
|_    421 No SMTP service here
80/tcp   open  http       Oracle GlassFish 5.0.1 (Servlet 3.1; JSP 2.3; Java 1.8)
|_http-server-header: GlassFish Server Open Source Edition  5.0.1
110/tcp  open  pop3?
| fingerprint-strings:
|   NULL:
|_    -ERR No POP3 service here
514/tcp  open  shell?
1720/tcp open  h323q931?
3306/tcp open  mysql      MySQL (unauthorized)
```

Anexo 56. Vulnerabilidades encontradas en el Servidor de Aplicaciones con la herramienta NMAP

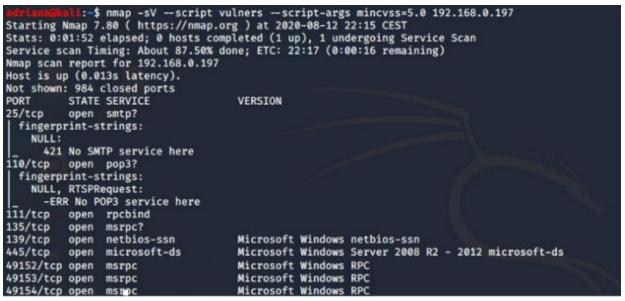


```
adriana@kali:~$ nmap -sV --script vulners --script-args mincvss=5.0 192.168.0.19
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-12 22:13 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.82 seconds
```

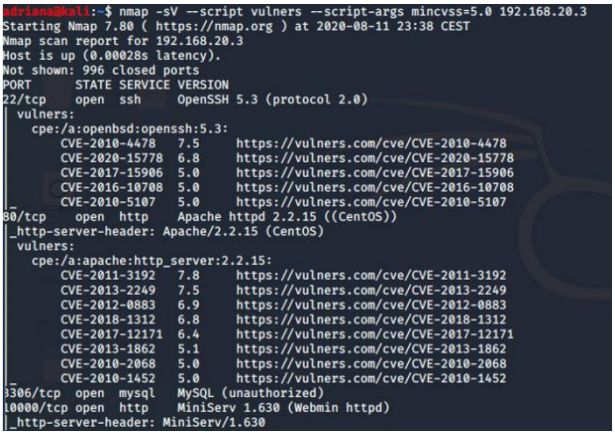
Anexo 57. Vulnerabilidades encontradas en el Servidor de Nómina con la herramienta NMAP



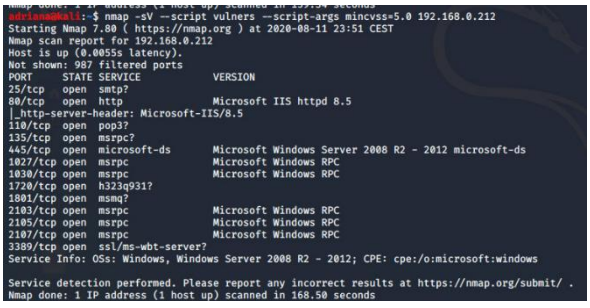
Anexo 58. Vulnerabilidades encontradas en el Servidor de Sistema Médico con la herramienta NMAP



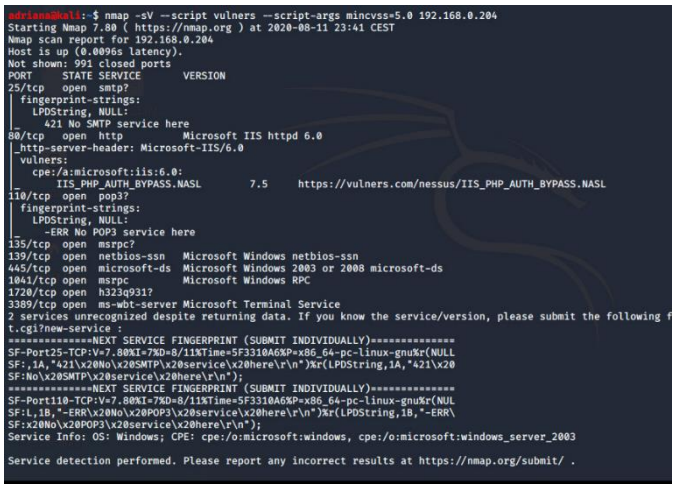
Anexo 59. Vulnerabilidades encontradas en el Servidor de Replicación con la herramienta NMAP



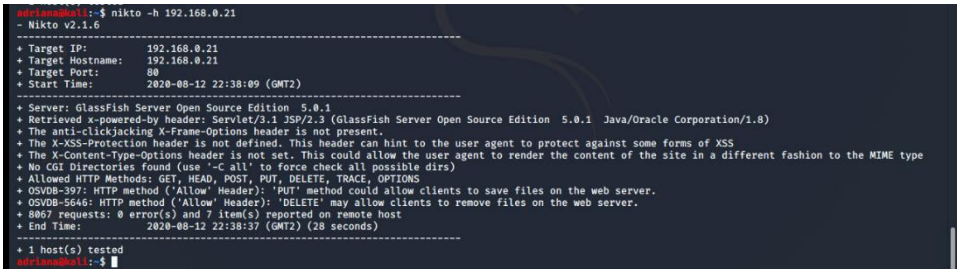
Anexo 60. Vulnerabilidades encontradas en el Servidor de Intranet con la herramienta NMAP



Anexo 61. Vulnerabilidades encontradas en el Servidor Web Services Produbanco con la herramienta NMAP



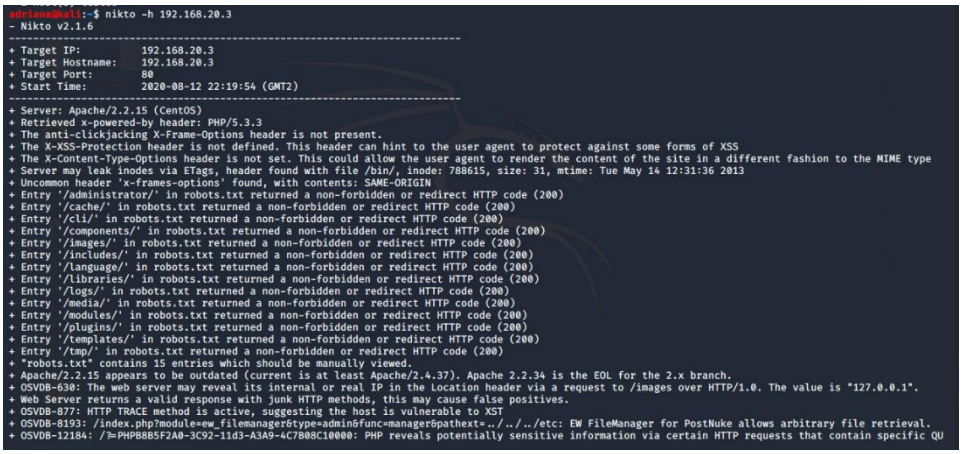
Anexo 62. Vulnerabilidades encontradas en el Servidor Web Services Equifax con la herramienta NMAP



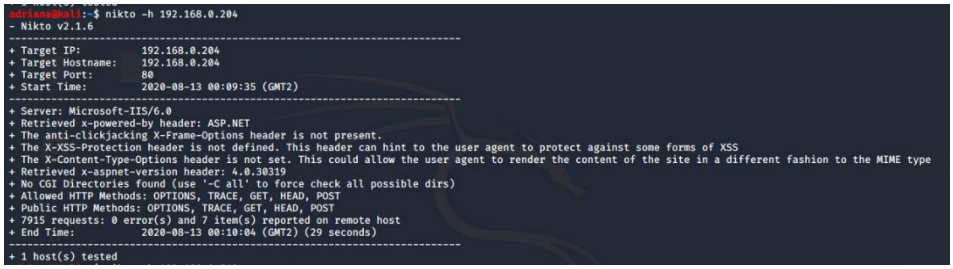
Anexo 63. Vulnerabilidades encontradas en el Servidor de Aplicaciones con la herramienta NIKTO

Anexo 64. Vulnerabilidades encontradas en el Servidor de Nómina con la herramienta NIKTO

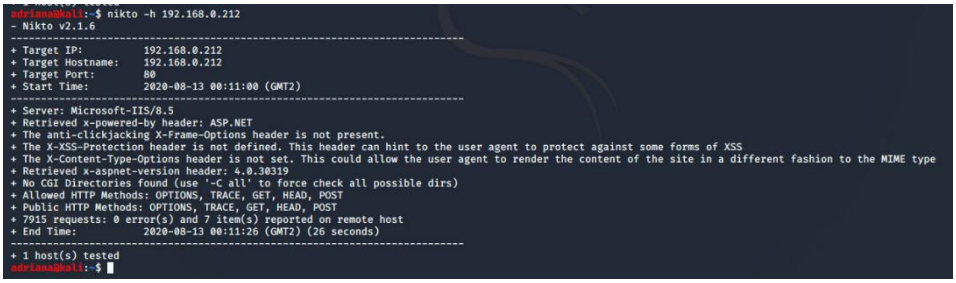
Anexo 65. Vulnerabilidades encontradas en el Servidor de Sistema Médico con la herramienta NIKTO



Anexo 66. Vulnerabilidades encontradas en el Servidor de Intranet con la herramienta NIKTO



Anexo 67. Vulnerabilidades encontradas en el Servidor Web Services Produbanco con la herramienta NIKTO



Anexo 68. Vulnerabilidades encontradas en el Servidor Web Services Equifax con la herramienta NIKTO